U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

June 8, 2016

MS. ALEXA O'BRIEN
MUCKROCK NEWS
DEPT MR 17650
POST OFFICE BOX 55819
BOSTON, MA 02205-5819

FOIPA Request No.: 1329073-000
Subject: Carnivore

Dear Ms. O'Brien:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act. Enclosed is one CD containing 605 pages of previously processed documents and a copy of the Explanation of Exemptions. Please be advised, these are the only copies of these documents located in our possession. The original copies of these documents could not be located for reprocessing.

Additional records potentially responsive to your subject exist. The Federal Bureau of Investigation (FBI) has located approximately 1,594 pages total of records potentially responsive to the subject of your request. By DOJ regulation, the FBI notifies requesters when anticipated fees exceed $25.00.

If all potentially responsive pages are released on CD, you will owe $40.00 in duplication fees (3 CDs at $15.00 each, less $5.00 credit for the first CD). Releases are made on CD unless otherwise requested. Each CD contains approximately 500 reviewed pages per release. The 500 page estimate is based on our business practice of processing complex cases in segments.

Should you request that the release be made in paper, you will owe $79.70 based on a duplication fee of five cents per page. See 28 CFR §16.10 and 16.49.

If you agree to receive all responsive material on CD, you will receive a $5.00 credit towards your first interim CD. As a result, we must notify you there will be a $25.00 charge when the second interim release is made in this case. At that time you will be billed for the $10.00 remaining from the $15.00 free of the first release, as well as the $15.00 duplication fee for the second release, for a total of $25.00.

Please remember this is only an estimate, and some of the information may be withheld in full pursuant to FOIA/Privacy Act Exemptions(s). Also, some information may not be responsive to your subject. Thus, the actual charges could be less.

Requester Response

No payment is required at this time. If your request does not qualify for eFOIA releases, you must notify us in writing within thirty (30) days from the date of this letter of your format decision (paper or CD). You must also indicate your preference in the handling of your request in reference to the estimated duplication fees from the following four (4) options:

☐ I am willing to pay estimated duplication/ international shipping fees up to the amount specified in this letter.

☐ I am willing to pay fees of a different amount.

Please specify amount: _____

☐ Provide me 100 pages or the cost equivalent ($5.00) free of charge. If applicable, I am willing to pay International shipping fees.

☐ Cancel my request.

If we do not receive your duplication format decision and/or estimated duplication fee selection within thirty (30) days of the date of this notification, your request will be closed. Include the FOIPA Request Number listed above in any communication regarding this matter.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You have the opportunity to reduce the scope of your request; this will accelerate the process and could potentially place your request in a quicker processing queue. This may also reduce search and duplication costs and allow for a more timely receipt of your information. The FBI uses a multi-queue processing system to fairly assign and process new requests. Simple request queue cases (50 pages or less) usually require the least time to process.

Please advise in writing if you would like to discuss reducing the scope of your request and your willingness to pay the estimated search and duplication costs indicated above. Provide a telephone number, if one is available, where you can be reached between 8:00 a.m. and 5:00 p.m., Eastern Standard Time. Mail your response to: **Work Process Unit; Record Information/Dissemination Section; Records Management Division; Federal Bureau of Investigation; 170 Marcel Drive; Winchester, VA 22602**. You may also fax your response to: 540-868-4997, Attention: Work Process Unit.

For questions regarding our determinations, visit the www.fbi.gov/foia website under “Contact Us.” The FOIPA Request number listed above has been assigned to your request. Please use this number in all correspondence concerning your request. Your patience is appreciated.

Carnivore. John Conyers, Democrat of Michigan.

Representative JOHN CONYERS (Democrat, Michigan): Constitutional rights don't end where cyberspace begins.

OSGOOD: And if the FBI is as scrupulous about using Carnivore as it says it is, there's always Murphy's Law to consider. That's the one that says, 'If anything bad can happen, it will.' Republican Congressman Spencer Bachus of Alabama.

Representative SPENCER BACHUS (Republican, Alabama): The potential for abuse here's tremendous.

OSGOOD: THE OSGOOD FILE. Charles Osgood on the CBS Radio Network.

LANGUAGE: English

LOAD-DATE: July 25, 2000

July 25, 2000, Tuesday

SECTION: GENERAL NEWS
LENGTH: 956 words
HEADLINE: On The Net
BYLINE: By United Press International
BODY:

Justice Department officials defended its "Carnivore" e-mail scanning program on Monday in front of a House panel, saying it is "narrowly focused" and they have used it just 25 times in two years, including 16 times so far this year. "Discriminating between users' messages on the Internet ... is exactly what Carnivore does," said Donald Kerr, assistant director at the FBI. "It does not search through the contents of every message and collect those that contain certain key words like 'bomb' or 'drugs.' It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user." Kerr told the House Judiciary Subcommittee on the Constitution that all but six uses of the program this year have been for "national security reasons," but he declined to talk about the cases. Attorney General Janet Reno has ordered an independent review of the system to determine whether it infringes on privacy rights. The American Civil Liberties Union has filed a Freedom of Information Act request with the department for all documents related to Carnivore. 0-

Another Internet file-trading service is facing a lawsuit by Hollywood heavy-hitters. Scour.com, a site that searches the Internet for music and video files and allows users to exchange them, is the target of a copyright infringement suit filed in New York by the Recording Industry Association of America and the Motion Picture Association of America. Scour.com, which is backed in part by former Disney head Michael Ovitz, said it was "very surprised" by the lawsuit, because the company had been in recent talks with top industry players such as Sony. MPAA Chairman Jack Valenti called the site "Napster with movies." 0-

The recording industry's case against Napster, meanwhile, goes to trial on Wednesday in San Francisco. Lawyers for the major record labels are expected to ask a judge to shut Napster down because it allegedly promotes music piracy and copyright infringement. Napster allows users to share MP3 digital recordings of songs that are compact-disc quality and can be downloaded in a few minutes. "The fact is that Napster has given millions and millions of music fans the opportunity to hear music they haven't heard before," said Napster CEO Hank Barry to the New York Times. Experts watching the case don't expect it to end quickly-the issues are complicated, and Napster has amassed a battled-hardened legal team on its side. 0-

Napster's case has recently drawn a lot of the media's attention, but the high-tech world's biggest case is still simmering in the background. A federal judge found in June that Microsoft had used illegal and unfair tactics to push its Windows operating system, and the company has one appeal left - to the Supreme Court. But the case might have one last detour. Microsoft wants to apply a federal antitrust law enacted in the 1970s that would allow a lesser court to hear the appeal first. According to the Washington Post, the company's lawyers believe the Supreme Court would benefit from another review of factual and procedural issues in the case. The government and the company can file more paperwork on the issue in August, and the Supreme Court could make a decision by the fall on whether it will hear the appeal. 0-

Stephen King said he offered his new serial novel "The Plant" on the Web for a "buck an episode" because he wanted to test how people would respond. "We have a generation of computer jockeys that we've raised on Napster and MP3

Doc. #38

who have gotten ... the mistaken idea that everything in the store is free. And I'd like to see if we can't reeducate these people to the idea that the fruits of talent cost you money," the author said Monday on ABC's "Good Morning America." Readers can download the first two portions of the book without paying the $1, but according to King on his Web site, "If you don't, the story folds." He wants 75 percent of all readers to pay for the story in order to keep it going. It's available at:
http://www.stephenking.com/download.html 0-

A French judge has ordered a series of tests into whether Internet screening software works well enough to require Yahoo! to block French Web surfers from having access to online auctions of Nazi memorabilia. French law prohibits the sale or exhibition of items with racist overtones, so a judge in June ordered the Web company to block access to the auctions. Because such auctions are legal elsewhere, Yahoo! only cut them from its France-oriented fr.yahoo.com site, not its main, global Yahoo.com portal. The company argued that it doesn't have the means to keep French users from accessing all the auctions outside of fr.yahoo.com, but Judge Jean-Jacques Gomez said that idea should be tested by experts before he makes another ruling in August. Yahoo! could face hundreds of thousands of dollars in fines. 0-

Rivals of America Online's instant messaging service have banded together in an attempt to get the Virginia company to open up its huge community of real-time Internet chatters. The MSN Network, AT&T Corp., iCast Corp. and Tribal Voice have formed a coalition called IMUnified that will push AOL to let them connect to its IM service, which has tens of millions of users. The group might end up with the government on its side - the IM issue is one of many that the Federal Communications Commission will consider on Thursday when it holds a hearing on the proposed AOL-Time Warner merger. IMUnified has an uphill battle ahead according to industry analysts. Mark Levit of International Data Corp. told Computerworld that AOL will only give in when it is certain its IM market share won't be affected. 0-

LANGUAGE: ENGLISH

LOAD-DATE: July 26, 2000

SHOW: MORNING EDITION (11:00 AM on ET)
July 25, 2000, Tuesday

LENGTH: 584 words
HEADLINE: FBI'S SYSTEM TO MONITOR E-MAILS GOING THROUGH INTERNET SERVICE PROVIDERS CALLED UNCONSTITUTIONAL BY MANY
ANCHORS: BOB EDWARDS
REPORTERS: LARRY ABRAMSON
BODY:

BOB EDWARDS, host:

The FBI is struggling to defend a controversial wiretapping system for the Internet. The system is called Carnivore. It's designed to help investigators search for evidence by sifting through huge volumes of e-mail. Civil liberties groups say Carnivore exposes law-abiding citizens to an FBI investigation. The FBI told members of Congress yesterday that the system can be trusted because it only examines messages relevant to investigations. NPR's Larry Abramson reports.

LARRY ABRAMSON reporting:

Usually the FBI asks Internet service providers to do its eavesdropping work, but if an ISP cannot supply the right information, the agency has been turning to Carnivore. Despite its ominous name, Carnivore is just a computer with special software. The FBI installs the system in the offices of the Internet service provider. Like a big vacuum cleaner, Carnivore sucks up every single e-mail message sent or received through the provider. But according to the FBI's Donald Kerr, Carnivore spits out everything except for the few bits that are related to the investigation.

Mr. DONALD KERR (FBI): What it's basically allowing us to do is record the address to which the envelope is being sent and the return address on the outside of the envelope. We're not permitted to read the subject line and, in fact, do not capture that and record it.

ABRAMSON: It's a lot harder for the FBI to get court authority to actually open up e-mail messages. The FBI assured members of a House Judiciary subcommittee that Carnivore software can be carefully tailored so that it only traps the names of the sender and the recipient of a message. Agents have used these kinds of searches on telephone lines for decades. Kevin Di Gregory, with the Department of Justice, says they're very useful in the early stages of an investigation.

Mr. KEVIN Di GREGORY (Department of Justice): To illustrate, law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products or to whom the drug dealer is selling his goods. It is, therefore, important to determine with whom the drug dealer is communicating.

ABRAMSON: The problem is that the system has to peek at each bit of information so that it can decide what to throw away. Many members of the Congress and civil liberties groups are not ready to trust the FBI when it says it really will discard information it's not allowed to collect. Barry Steinhardt of the American Civil Liberties Union called the potential for abuse unprecedented.

Mr. BARRY STEINHARDT (American Civil Liberties Union): Never before has law

DOC. #39

enforcement installed a device which access all the communications of a service providers customers rather than only the communications of the target of a particular order.

ABRAMSON: Internet service providers have become accustomed to court orders and subpoenas for information in criminal investigations and lawsuits. But many say they resent the FBI's use of Carnivore. They say the system poses a security threat and can crash an ISP's computers. Congressman Bob Barr of Georgia accused the agency of abusing its authority and bullying its way on to the premises of Internet service providers.

Representative BOB BARR (Georgia): You're saying, 'What we're going to do is we're going to go outside of the law here basically and we're going to force you to allow us to put our software into your system. You will not be able to monitor it. It's completely unsupervised. Thank you very much, guys. You just give us access and we'll do our thing.'

ABRAMSON: Much of the Carnivore debate hinges on just what Internet users expect when they send e-mail. Courts have ruled that telephone callers have no right to expect that the telephone numbers they dial will be kept private. But Stuart Baker, former general counsel at the National Security Agency, says extending that analogy to Internet service providers doesn't make sense.

Mr. STUART BAKER: To say you don't have an expectation of privacy in information that is in the hands of the third party in the Internet age is just crazy. I mean, our entire lives are in the hands of third parties.

ABRAMSON: The FBI is offering to hire an independent investigator to prove that Carnivore offers a constitutional way to wiretap on the Internet. But so far, the agency says it will not reveal the software code behind the system. Many civil libertarians say that's the only way they can prove to Congress that Carnivore is dangerous and should be abandoned. Larry Abramson, NPR News, Washington.

LANGUAGE: English

LOAD-DATE: August 7, 2000

Chicago Tribune

July 25, 2000 Tuesday, CHICAGO SPORTS FINAL EDITION

SECTION: News; Pg. 1; ZONE: N
LENGTH: 989 words
HEADLINE: FBI DEFENDS USE OF E-MAIL MONITORING SOFTWARE
BYLINE: By Frank James, Washington Bureau.
DATELINE: WASHINGTON
BODY:

Privacy experts and lawmakers on Monday criticized the FBI for using technology that monitors e-mail, claiming that it threatens privacy rights. But computer security experts say those concerns miss the point: By its very nature, e-mail is not secure. Electronic messages are among the worst ways to send private information.

Speaking after a House Judiciary subcommittee hearing Monday, Tom Perrine, a computer expert, lamented that he ran out of time before he could explain to lawmakers that it's not just government snoops using a special, secret software program like "Carnivore" that threaten e-mail privacy.

Anyone with a little computer know-how can catch and read other people's online mail. The answer, he and other experts say, is a simple encryption program that codes the e-mail so others can't read it.

"If everyone used strong encryption, large parts of Carnivore would be completely useless," Perrine said.

At the 3 1/2-hour hearing, Democratic and Republican skeptics openly doubted the FBI's ability to keep from abusing its Carnivore technology and violating Americans' constitutional rights with the Internet equivalent of a telephone wiretap.

For two years, witnesses testified, the agency has quietly used Carnivore to capture the "to" and "from" lines of e-mail between certain suspects and their e-mail buddies. When federal judges have provided the agency with the required authority, the FBI also has captured not just the address information, but the content of targeted e-mails.

Privacy experts, lawmakers and others have sharply criticized the FBI for its use of the program; Monday's hearing was filled with accusations of privacy violations.

"I think Congress has to act," said Rep. Jerrold Nadler (D-N.Y.), calling for tighter restrictions on the FBI. "Police agencies can't be afforded untrammeled discretion, and we can't assume a lack of bad intent on the part of police or the presence of goodwill is enough to protect people's privacy."

The FBI's general counsel, Larry Parkinson, assured the lawmakers: "There are checks and balances with respect to Carnivore. ... It's not a situation where a rogue FBI agent could broaden the coverage of the Carnivore intercept and violate the court order" authorizing the surveillance.

What the numerous witnesses defending the use of Carnivore, as well as privacy advocates condemning it, didn't acknowledge, however, was the thing they all agree on--the insecurity of e-mail in general.

President Clinton knows. After a speech last March in Silicon Valley, as reported by Dan Gillmor, technology columnist for the San Jose Mercury News, someone asked Clinton if he keeps in touch with his college student daughter, Chelsea, by e-mail while she is away at Stanford University.

Doc. #40

"I don't do e-mail with Chelsea. Absolutely not--I don't think it's secure," said Clinton.

Indeed, said Perrine, manager of security technologies at the San Diego Supercomputer Center, at the University of California-San Diego, everyone worries about protecting their computers, but too many send sensitive information by e-mail.

"There's a quote, I wish I could remember who said it, but basically it goes ... 'Trying to do secure things over the Internet is like two people in concrete bunkers surrounded by machine guns sending messages to each other written on the back of postcards,'" Perrine said.

"There's all this communication that goes across that can be read by anyone" with access to the network and technology called a packet sniffer, he said.

E-mail transmitted over the Internet, like all information sent over the global network, is broken into chunks called packets that are bounced from the sender's computer to the recipient's. Because of the way the Internet was constructed, the packets often take different routes to get from point A to point B, bouncing around the Internet until they arrive at their destination and are reassembled.

At the right place on the network, a hacker or someone else using a packet sniffer can collect the packets then reassemble them to learn the contents of an e-mail, leading to the security issue Clinton raised.

The greatest cause for concern is the possibility of an inside job, someone with access to the powerful computers known as servers, the brains of computer networks, said Richard Smith, an Internet security expert based in Cambridge, Mass.

"In the case of Chelsea, the concern I would have as President Clinton or the Secret Service is that somebody at Stanford, or wherever, who maintains the e-mail system was watching that traffic, that they got $10,000 from a tabloid [newspaper] to read those e-mails and spy on Chelsea for whatever reason," he said.

Sensitive corporate information and trade secrets are equally vulnerable when they are mentioned in e-mail, which has its roots in an easy-to-read format.

"If anything cried out for being encrypted, I would say e-mail does," Smith said. "Maybe over time, that can be a change that happens."

Actually, powerful encryption tools are currently available to virtually all computer users, though they take some knowledge of computers to properly employ.

Computer experts foresee growing consumer demand for encryption. "We can expect that as people learn that e-mail is not secure, there'll be more interest in using encryption to protect it," said Matt Blaze, a research scientist with AT&T Labs. "Most people now don't use it because they're not interested in it or it's not available to them in the standard configuration that comes with their computer."

Perrine said an Internet engineering standards group recently developed guidelines that could hasten the day when people routinely send encrypted e-mail messages.

"All traffic between cooperating computers would be encrypted and in most cases this would be transparent to the user," he said. "Those technologies, if they're not already here, are at least on the horizon."

LANGUAGE: ENGLISH

LOAD-DATE: July 25, 2000

July 25, 2000

SECTION: EDITORIAL
LENGTH: 601 words
HEADLINE: E-mail's big brother
BYLINE: Staff Editorial, Michigan Daily
SOURCE: U. Michigan
DATELINE: Ann Arbor, Mich.
BODY:

The FBI has recently come under fire from internet privacy groups and the ACLU for a controversial e-mail snooping system that monitors all e-mail passing through networks connected to the device. The system, dubbed "Carnivore" by the FBI -- because it gets at the "meat" of information -- is dangerous because it is capable of scanning sender and receiver information along with the subject lines of all passing mail to determine if those messages contain information worth saving for FBI review. Unlike phone taps, Carnivore's almost unlimited access to private messages carries a high potential for abuse by overzealous FBI agents and allows the possibility of targeting users not suspected of any crime.

Court orders are currently required to tap phone lines or gather information from ISP's on possible illegal activity carried out over electronic mediums like e-mail, but Carnivore is much more pervasive. The system is an untouchable box installed on private networks to collect all information passing through them. This is like installing a device that listens to every phone conversation to determine whether or not the phone calls should be monitored by law enforcement. But information on the inner workings of Carnivore remains sketchy. This alarms many privacy advocates, like Representative Bob Barr (R-GA), who had one word for the system: "Frightening."

One solution involves allowing the code of Carnivore to be perused by independent groups who would examine its workings to make sure the information being collected is limited to those under investigation for illegal activity. This seems a viable solution, as the integrity of the Carnivore system would not be violated, yet could still be monitored. The FBI announced Friday that Carnivore could be reviewed by independent academics, but this does not go far enough.

A more palatable alternative to Carnivore would leave ISP's responsible for turning over information on targeted users for FBI review, as is the current practice with phone companies in possession of incriminating evidence. This allows some degree of protection and would be a reasonable alternative to widespread electronic surveillance.

More sweeping reform could come from Congress, as legislators examine the ACLU's recommendation to draft legislation that would bring Carnivore and similar schemes under control. Current privacy legislation needs to evolve to include provisions ensuring that access to electronic communications by law enforcement is limited to suspect users and specific court-approved targets only. The potentially abusive nature of Carnivore is not something we should learn to live with in the digital age. Law-abiding citizens cannot have their privacy infringed by law enforcement agencies interested in collecting data on a few criminals.

Congress must keep up with the times and fully examine the feasibility of wide-ranging changes to electronic privacy. Outdated laws like the 14-year-old Electronic Communications Privacy Act, which allows for real-time interception of messages with a court order, does not include provisions for new technologies and allows for loopholes like Carnivore.

Doc #41

Whether Carnivore's code is opened to public investigation or more stringent attention is paid to governmental bodies engaged in electronic snooping, the laws are far behind technological means. It is time the American people receive comprehensive legislative protection from risky, unaccountable law enforcement techniques that violate Fourth Amendment protection from unreasonable searches.

LANGUAGE: ENGLISH

LOAD-DATE: July 25, 2000

The Washington Post

July 25, 2000, Tuesday, Final Edition

SECTION: FINANCIAL; Pg. E01
LENGTH: 704 words
HEADLINE: FBI Makes Case For Net Wiretaps; 'Carnivore' System Faces Fire on Hill
BYLINE: John Schwartz , Washington Post Staff Writer
BODY:

Federal law enforcement officials defended "Carnivore"--the FBI's controversial Internet wiretap system--through more than two acrimonious hours of grilling by Democratic and Republican lawmakers yesterday, painting a chilling picture of an Internet that would become a safe haven for crooks and terrorists without proper surveillance.

"Criminals use computers to send child pornography to each other using anonymous, encrypted communications," FBI Assistant Director Donald M. Kerr told the House Judiciary subcommittee on the Constitution. "Hackers break into financial service companies' systems and steal customers' home addresses and credit-card numbers, criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world, and terrorist bombers plan their strikes using the Internet."

Many of the lawmakers seemed just as concerned with the actions of the law enforcement officials. "The potential for abuse here is tremendous," said Rep. Spencer Bachus (R-Ala.). "What you're saying is 'Trust us.' "

Carnivore is a modified version of a common network-maintenance program known as a "packet sniffer." Carnivore offers great specificity--the ability to quickly collect just the "to" and "from" information in e-mail messages, for example, and not online banking transactions. That gives law enforcement the equivalent of the telephone world's "pen register" and "trap and trace" data--the origin and destination of all calls related to the subject.

Civil liberties groups and Internet service providers say the system raises troubling questions about what constitutes a reasonable search and seizure of electronic data. In sniffing out potential criminal conduct, they note, the new technology also could scan private information about legal activities, taking in vast amounts of information from innocent people as well as the suspect.

The critics also note that past experience has shown that law enforcement has overstepped its wiretap authority numerous times in the past.

Barry Steinhardt, associate director of the American Civil Liberties Union, said in his testimony: "Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all the phone company's customers, with the 'assurance' that the FBI will record only conversations of the specified target."

Officials of Internet service providers who oppose the technology say they are wary of putting equipment designed by others on their networks. They want the FBI to publish information on the software used so that ISPs can be sure that it does what the agency says.

The law enforcement officials pledged to present the system to a neutral third party for review but said they cannot release so much information about the system that it will become a target for evasion and hacking.

They insisted the Carnivore system actually provides greater privacy than previous methods of gathering electronic information because it can fine-tune what the machine hands over to investigators.

Doc. #42

The FBI's Kerr also argued that agents won't "risk their integrity, their jobs and their futures" by abusing the law.

The toughest questioning came from Reps. Jerrold Nadler (D-N.Y.) and Robert L. Barr Jr. (R-Ga.), two congressmen rarely on the same side of an issue. Nadler peppered the officials with a series of questions that underscored the point that Carnivore, under the laws that govern pen-register surveillance, could be used without the difficult showing of "probable cause" required in a telephone wiretap.

Barr cited the investigation of missing White House e-mail and scornfully said the Clinton administration asserts that "we don't even know how to keep track of our own e-mail" while "now we see a very sophisticated system for keeping track of other people's e-mails!"

After the hearing, House Majority Leader Richard K. Armey issued a statement saying members of both parties showed "strong concerns that the administration is infringing on Americans' basic constitutional protection against unwarranted search and seizure.

"Until these concerns are addressed," he concluded, "Carnivore should be shut down."

LANGUAGE: ENGLISH

LOAD-DATE: July 25, 2000

The Washington Times
July 25, 2000, Tuesday, Final Edition

SECTION: PART A; Pg. A1
LENGTH: 744 words
HEADLINE: Lawmakers rip FBI e-mail tracker;
Surveillance tool employed 25 times
BYLINE: William Glanz; THE WASHINGTON TIMES
BODY:

Federal law enforcement agents say they have used the controversial Carnivore software program to track e-mail of suspects 25 times in the past two years.

But agents have never used the program illegally or tracked e-mail they were not authorized to track by a court order, FBI Assistant Director Donald Kerr told the House Judiciary subcommittee on the Constitution yesterday.

Despite the restraint the FBI says it has used, privacy rights advocates criticized law enforcement agents for using Carnivore and lawmakers expressed skepticism about the federal government's use of the Internet surveillance tool.

House Majority Leader Dick Armey, Texas Republican, said yesterday Carnivore should be suspended until concerns of privacy advocates and needs of law enforcement are reconciled.

"Until these concerns are addressed, Carnivore should be shut down," he said.

Carnivore enables investigators to pick out specific e-mail messages traveling through an Internet service provider's computer system so it can monitor who a suspect contacts and who contacts a suspect.

Mr. Kerr and other federal officials said the high-tech surveillance system is crucial to help them keep up with an increasingly sophisticated breed of tech-savvy criminals and crucial to help them keep the Internet safe.

"Many of the crimes that we confront every day in the physical world are beginning to appear on line," said Deputy Assistant Attorney General Kevin DiGregory.

"If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the information age. . . . Carnivore is simply an investigative tool that is used on line only under narrowly defined circumstances and only when authorized by law to meet our responsibilities to the public," he said.

But lawmakers expressed concern about a lack of checks and balances on law enforcement agents using Carnivore.

"The potential for abuse here is enormous," said Rep. Spencer Bachus, Alabama Republican.

FBI General Counsel Larry Parkinson said Carnivore is a little-used tool. When it is used, Mr. Kerr said, agents follow the law carefully, and if they are caught collecting more data than allowed, they can be imprisoned up to five years for committing a federal felony.

"In the past, we've had many agencies go beyond the scope of their authority," said Rep. John Conyers Jr., Michigan Democrat.

Mr. Kerr said the FBI and Department of Justice will seek an independent

Doc. #43

review of Carnivore this year to show they aren't misusing the program.

Lawmakers and privacy rights advocates also criticized federal officials for using Carnivore when Internet service providers could just as easily collect information being sought.

"There ought to be more control in the hands of the Internet service providers ," said Alan Davidson, a lawyer with the District-based civil liberties group Center for Democracy and Technology.

Mr. Kerr argued that few of the nation's estimated 10,000 Internet service providers have the means to sift through e-mail traffic and collect them for law enforcement.

But Robert Corn-Revere, an attorney who represented Atlanta-based Internet service provider EarthLink, said EarthLink was gathering e-mail information at the federal government's request earlier this year when it was forced to comply with a court order and let federal officials install Carnivore on its computers.

The federal government was upset that EarthLink was capturing few e-mail messages, Mr. Corn-Revere said, and it needlessly installed Carnivore.

American Civil Liberties Union Associate Director Barry Steinhardt suggested Carnivore's source code be made public. The source code is the set of instructions a programmer writes, and it will show just what Carnivore is capable of retrieving. The ACLU has filed a Freedom of Information Act request with the FBI to get the source code.

Even though they had a raft of questions about Carnivore and its use, lawmakers yesterday didn't express any willingness to make immediate changes in the federal government's authority to use the surveillance program.

"We should be sensitive to any potential for abuse of the Carnivore system. Even a system designed with the best of intentions to legally carry out essential law enforcement functions may be a cause for concern if its use is not properly monitored," said Rep. Charles T. Canady, Florida Republican.

LANGUAGE: ENGLISH

LOAD-DATE: July 25, 2000

SHOW: CBS MORNING NEWS (6:30 AM ET)
July 25, 2000, Tuesday

TYPE: Newscast
LENGTH: 388 words
HEADLINE: NEW SURVEILLANCE SOFTWARE ALLOWS THE FBI TO SNOOP THROUGH COMPUTER USERS' E-MAILS
ANCHORS: SHARYL ATTKISSON
REPORTERS: JIM STEWART
BODY:

SHARYL ATTKISSON, anchor:

First came wiretapping phones. Now the FBI is using a controversial cybersurveillance program called Carnivore that wiretaps the Internet. Jim Stewart reports.

JIM STEWART reporting:

Every day, more than a billion e-mails are sent and received by computer users, and the FBI thinks criminals are now just as fond of them as the next guy. But the problem for agents has always been: Just how do you sort through all the gibberish to find any meaningful evidence? The bureau told Congress it thinks it's found the answer in a software program called Carnivore.

Mr. LARRY PARKINSON (General Counsel, FBI): This is--despite its unfortunate name, this is a tool that is very surgical.

STEWART: Essentially, Carnivore is like a wiretap on the Web. Physically, it's nothing more than a small computer the FBI can lock inside the switching room of an Internet service provider like, say, America Online. But instead of reading every AOL customer's e-mail, it's designed to zero in and record just the messages sent to and from one particular e-mail address.

Mr. DONALD KERR (Director, Lab Division, FBI): We don't do broad searches or surveillance with this system. That's not authorized by a court order and, in my view, could not be.

STEWART: Critics, however, immediately asked: Who's watching the watchers?

Mr. ALAN DAVIDSON (Center for Democracy & Technology): Carnivore has access to much more information than it is legally entitled to collect. How do we know that we can trust Carnivore? How do we know what kind of leash has been put on Carnivore?

STEWART: The reason for the skepticism is because there's a big difference between wiretapping the Internet and wiretapping a telephone. If the FBI wants to bug your telephone, they get a court order and go to the phone company, and the phone company makes the connection for the bureau. If the FBI wants to wiretap your Internet address, they get a court order and then they can make the connection themselves.

They've done it 16 times this year already, mostly against Internet hackers, and the potential list of suspects and their crimes is growing, agents warned. Four years from now, the number of commercial e-mail messages alone is expected to top 200 billion a year. Jim Stewart, CBS News, Washington.

LANGUAGE: English

LOAD-DATE: July 25, 2000

Doc. #44

SEATTLE POST-INTELLIGENCER

July 25, 2000, Tuesday

SECTION: NEWS,
LENGTH: 664 words
HEADLINE: FBI ACCUSED OF VIOLATING E-MAIL PRIVACY;
ADVOCATES SAY PROGRAM SIFTS THROUGH EVERY FILE SENT THROUGH SPECIFIC ISPMARK HELM P-I WASHINGTON BUREAU
DATELINE: WASHINGTON
BODY:

Privacy advocates and technology experts yesterday blasted a new FBI program to police the Internet, saying the system allows agents to monitor e-mails of people who are not targets of criminal investigations.

"The FBI asks you to trust them with unsupervised access . . . to literally millions of innocent communications," Barry Steinhardt, associate director of the American Civil Liberties Union, told a House subcommittee investigating the system. "For me, that's an enormous leap of faith that the public is being asked to take."

The e-mail sniffing system, known as "Carnivore," allows law enforcement officials to sift a suspect's messages out of the full stream of data passing through an Internet service provider (ISP), like America Online.

Once installed on the ISP network, Carnivore can monitor all of the e-mail on that ISP, from the list of what is sent to the actual content of the e-mail.

Steinhardt told the subcommittee on the Constitution that Carnivore differs significantly from traditional phone wiretaps. With a phone wiretap, the FBI must obtain a court order to monitor conversations of a specific phone. Then, the FBI contacts the phone company, which installs the tap, and, when the investigation ends, disconnects it. Agents are not able to monitor any conversations other than those on the one phone.

Under the Carnivore system, the FBI first gets a court order to use the agency's software to tap into the lines of an ISP. Unlike a traditional wiretap with access to only one phone, Carnivore has access to every message being sent along the ISP's system. In addition, the ISP has no control over or knowledge of what the FBI is monitoring.

Peter Sachs, president of ICONN, a New Haven, Conn.-based ISP, said Carnivore violates the rights of every "law-abiding" citizen who uses the Internet to send e-mail.

"At this very moment, a government-controlled computer, installed under court order at some ISP somewhere in this country is busy reviewing all communications passing through that ISP, including messages from and to you, the members of Congress."

Sachs said the software used for Carnivore, which is secret, also poses other threats to Internet users. First, he said, the software could be vulnerable to hackers. Another problem, he said, is that the Carnivore already has caused service problems for several ISPs, causing them to stop or slow down.

But Justice Department and FBI officials said they are simply trying to preserve their ability to monitor criminal activity. They said that capability is being eroded by the growing use of new technologies such as encryption, cell phones and wireless message devices.

Kevin DiGregory, deputy associate attorney general, said Carnivore actually protects privacy because it can be configured to identify only the senders and

Doc. #45

recipients of the suspect's e-mail. The system selects only the data related to the criminal suspect, he said, so that human reviewers see only what the machine has culled.

"It's not just a situation where, as I understand it, a rogue FBI agent, for example, could broaden the coverage of the Carnivore intercept and violate the court order," DiGregory said. "In order to do that, he would need to engage the aid of technical people, perhaps even technical people at the Internet service provider."

Donald Kerr, director of the FBI's computer lab division, said Carnivore is used only when an ISP cannot provide the information requested under a court order. "The FBI would prefer to let ISPs do this work, but sometimes that's not possible and in those cases, we bring in Carnivore," he said.

Existing laws are ambiguous about what standards apply for different kinds of Internet surveillance.

Last Monday, the White House announced the administration will propose legislation to "harmonize" the laws of wiretapping as it affects the many technologies by which people communicate - such as telephone, dial-up modem and high-speed broadband access.

LANGUAGE: ENGLISH

LOAD-DATE: July 26, 2000

Newsbytes

July 27, 2000, Thursday

LENGTH: 481 words

HEADLINE: GOP Lawmakers Want To Starve "Carnivore"

BYLINE: David McGuire; Newsbytes

DATELINE: WASHINGTON, D.C., U.S.A.

BODY:

A powerful cadre of House Republicans today demanded that the FBI pull the plug on its controversial e-mail surveillance device, "Carnivore."

"Given the uproar Carnivore has created, and the potential impact reports on Carnivore could have on consumer confidence in the Internet, we urge you to suspend any activity involving the development or use of Carnivore until the serious privacy issues involved have been satisfactorily answered," the lawmakers wrote in a sternly worded letter to Attorney General Janet Reno.

Signed by 27 House Republicans including Majority Leader Dick Armey, R-Texas, and Majority Whip Tom DeLay, R-Texas, today's letter is aimed at forcing the Justice Department to move quickly in addressing the constitutional concerns raised by the FBI's use of the controversial device, Armey staffer Richard Diamond told Newsbytes today.

Designed to attach directly to an Internet service provider's internal systems, Carnivore is capable of sifting through vast quantities of e-mail messages to find those that meet investigative specifications of a court order. Messages that don't meet the specific parameters of a given court order are - according to the FBI - never read.

But the revelation that the FBI is sifting through millions of innocent Internet users' e-mail messages has spawned a groundswell of opposition to the device. Conservatives and liberals alike have decried the FBI's use of the device, claiming that using the technology violates constitutionally protected privacy rights.

"You shouldn't be using this kind of (technology) with this type of question hanging over your head," Diamond said.

The authors of today's letter asked Reno to retire the device until the FBI and Justice Department can adequately address the privacy concerns it raises. However, Reno, in her weekly Justice Department news briefing, said she would not suspend use of the device until after an internal FBI review of Carnivore is completed.

Diamond conceded that it is probably unlikely that Carnivore would ever meet with congressional approval. "The burden of proof is on the Attorney General to show us that (Carnivore) is in full compliance with the Fourth Amendment," Diamond said.

And at least one signatory to today's letter doesn't intend to wait for the Justice Department to shelve Carnivore of its own volition.

Rep. Bob Barr, R-Ga., is crafting legislation that would prevent the FBI from using Carnivore and devices like it, Barr staffer Brad Alexander said today.

The Justice Department was not available for comment on today's letter.

Doc. # 46

Earlier this month, Reno promised to personally investigate the FBI's use of Carnivore.

Reported by Newsbytes.com, http://www.newsbytes.com .

16:31 CST Reposted 16:31 CST

(20000727/WIRES ONLINE, LEGAL, BUSINESS/FBI/PHOTO)

LANGUAGE: ENGLISH

TYPE: NEWS

LOAD-DATE: July 28, 2000

Newsbytes

July 27, 2000, Thursday

LENGTH: 516 words

HEADLINE: Privacy Legislation Won't Move This Year - Leahy

BYLINE: David McGuire; Newsbytes

DATELINE: WASHINGTON, D.C., U.S.A.

BODY:

While broad-based Internet privacy legislation probably won't go very far in this congressional session, lawmakers are making progress on the thorny issue and will ideally be ready to develop something substantive next year, Sen. Patrick Leahy, D-Vt., told reporters and high- tech industry leaders today.

"I don't think anything will be done significantly this year," Leahy said, adding that Congress should begin working in earnest on setting baseline federal privacy standards next year, after the presidential election brouhaha has a chance to die down.

Despite the difficulty of establishing substantive privacy legislation in this Congress, Leahy blasted the notion of punting the privacy issue to a congressionally appointed panel.

"If we've got time to investigate the investigations of (Clinton Administration scandals) we ought to at least find the time to do something real-world" on privacy, Leahy said.

Pending House legislation would establish a commission to delve into the Internet privacy issue.

Although industry leaders remain leery of accepting federal Internet privacy standards without a fight, the business community's growing willingness to at least discuss a legislative remedy should help clear the way to enacting privacy legislation, Leahy said.

Leahy spoke today at a breakfast meeting on Capitol Hill where the Business Software Alliance (BSA) honored him with a "Cyber Champion Award." BSA, which represents a slew of large software makers - including Microsoft Corp. - doles out the Cyber Champion statuettes to lawmakers and regulators who support intellectual property and anti-piracy causes.

In addition to his work in the privacy arena, Leahy has played key roles in combating software piracy and supporting the relaxation of US export controls on encryption products. BSA leaders said that they gave Leahy the award to thank him for his work in those areas.

Following the meeting, BSA president Robert Holleyman told Newsbytes that while the software industry does not openly endorse the creation of federal privacy standards, the group would be open to discussing limited legislation with Leahy and his colleagues next year.

"It is premature to do something in Congress this year," Holleyman said. But BSA and its member companies would be willing to talk about endorsing strictly limited federal privacy legislation - particularly if such legislation would preempt harsher state and local measures.

Still, BSA wants Congress to give industry self-regulation a chance and

Doc. #47

Holleyman remains concerned that any privacy bill may go too far for his taste.

"Something might get started in that process that just becomes a snowball," Holleyman said.

During his remarks today, Leahy also addressed "Carnivore," the FBI's controversial e-mail surveillance device. "I don't think we are doing adequate oversight on Carnivore," Leahy said.

Reported by Newsbytes.com, http://www.newsbytes.com .

14:15 CST

(20000727 /WIRES ONLINE, LEGAL, BUSINESS/PRIVACYDOME/PHOTO)

LANGUAGE: ENGLISH

TYPE: NEWS

LOAD-DATE: July 27, 2000

The New York Times

July 27, 2000, Thursday, Late Edition - Final

SECTION: Section A; Page 24; Column 1; Editorial Desk

LENGTH: 635 words

HEADLINE: Wiretapping in Cyberspace

BODY:

Millions of Americans now log on to the Internet as naturally and as frequently as they pick up a phone. Technology has created a revolution in personal communications, but technology is also making it possible for government and even employers to monitor private conversations as never before. Telephone-era laws must be updated to address these new challenges to privacy.

Last week the White House proposed some limited changes to the federal wiretap and electronic privacy laws that would raise legal standards for government interception of e-mail. Separately, several lawmakers introduced legislation to require employers to notify employees about how e-mail, Internet use and phone calls are monitored. Employees of The New York Times Company are already notified that the company reserves the right to review e-mail messages while investigating a complaint. Last year the company dismissed 23 employees -- most based at a regional business office -- for sending offensive e-mail messages.

In the absence of more stringent controls, law enforcement agencies may be tempted to conduct wholesale monitoring of digital written communications. It is probably not practical for agents to listen in on all the phone calls, for example, that go through AT&T. But new technology is making it possible for agencies like the F.B.I. to scan, read and record millions of pieces of e-mail on the network of an Internet service provider. Until now, this kind of power and its potential for abuse were not so readily available.

Current wiretapping laws were not drafted with this technology in mind and need to be updated. Various statutes now set different legal standards for the secret interception of domestic communications by law enforcement agencies, depending on whether the communication is by telephone, e-mail or cable modem.

The Clinton administration is proposing to eliminate these inconsistencies. Its plan would bring the standards used for intercepting e-mail messages up to the stricter, more protective level now applied to telephone wiretaps. Illegal interception of e-mail would result in suppression of the evidence, as is the case now with illegal interception of phone calls. The proposal would also enforce the same legal standards that apply to phone calls for interception of e-mails sent by cable modems, which have a greater degree of privacy protection under a law that governs cable systems.

The administration is also calling for greater authority for courts to review law enforcement requests to use devices that record the phone numbers of incoming and outgoing calls and to track the origins and destinations of e-mail messages.

These changes are clearly needed. But Congress also needs to provide new safeguards against the government's wrongful use of ever more powerful surveillance technology against law-abiding citizens. Serious concerns have been raised about Carnivore, the new online wiretap system used by the F.B.I.

Doc. #48

to track the communications of individuals suspected of criminal activity.

The F.B.I. says the technology can isolate the e-mail of the target of an investigation. But the system, when hooked up to the network of the Internet service provider, gives the F.B.I. unlimited access to the e-mail of all other subscribers on the network. While a court order is still required to intercept the content of messages, the secret technology controlled exclusively by law enforcement raises fears of improper monitoring.

Until now, routine government surveillance of private conversations was limited as much by practicality as by legal constraints. Now that it is feasible to eavesdrop electronically on an unlimited scale, the laws have to be strengthened to prevent monitoring of all online communications simply because technology makes it easy.

http://www.nytimes.com

LANGUAGE: ENGLISH

LOAD-DATE: July 27, 2000

July 27, 2000, Thursday

SECTION: PRESS RELEASE
LENGTH: 478 words
HEADLINE: REP. CANADY INTRODUCES BILL TO UPDATE WIRETAP LAWS
BYLINE: CHARLES T. CANADY , REPRESENTATIVE , HOUSE

BODY: For immediate Release July 27, 2000 Rep. Canady Introduces Bill to Update Wiretap Laws E-Mails and Stored Internet Communications Would Be Covered WASHINGTON, D. C. - Rep. Charles T. Canady (R-FL), Chairman of the House Judiciary Subcommittee on the Constitution, today introduced the Electronic Communications Privacy Act of 2000. The bill would update the federal wiretap laws to cover e-mail and stored electronic communications, as well as provide special requirements for government tracing of e-mail addresses. Canady is joined by original cosponsor Rep. Asa Hutchinson (R-AR). "This legislation helps move our federal wiretap laws into the 21st Century," Canady said. "We have entered a new age with the Internet, and we need a new law to reflect the rapid changes in technology. While this legislation does not answer all the difficult issues raised by recent technological advances, it does provide for some reasonable reforms that will protect the privacy rights of Americans." Earlier this week, Rep. Canady chaired a Constitution Subcommittee hearing on Fourth Amendment issues raised by the FBI's "Carnivore 11 program. The FBI designed and developed Carnivore to isolate, intercept and collect communications that are the subject of lawful court orders. The July 24th hearing featured witnesses from law enforcement, civil liberty organizations, privacy organizations and representatives from the business community. BILL SUMMARY The Electronic Communications Privacy Act of 2000 has three sections. The first section amends the "statutory exclusionary rule" to also exclude from use as evidence illegally intercepted "electronic communications" and illegally obtained "stored electronic communications."

The bill simply adds electronic communications to the previously covered wire and oral communications. The second section of the bill requires the federal government to produce annual reports regarding its requests for orders for the disclosure of "stored electronic communications." This reflects virtually identical disclosure requirements the federal government must meet regarding the use of electronic wiretaps. The final section of the legislation amends the definition of "pen register" and "trap and trace" devices, defining them to allow the identification of an "e -mail address." In addition, the section requires that, if a pen register or trap and trace device is used to identify an e-mail address, the federal government must first demonstrate to a court that "specific and articulable facts reasonably indicate that a crime has been, is being, or will be committed, and information likely to be obtained by such installation and use {of a pen register or trap and trace device} is relevant to an investigation of that crime." For a copy of Rep. Canady's legislation (7pages) please call Michelle Knott at (202) 22-5-1252.

LANGUAGE: ENGLISH
LOAD-DATE: July 31, 2000, Monday

Copley News Service

July 27, 2000, Thursday

SECTION: Commentary

LENGTH: 396 words

Doc. #49

HEADLINE: Gobbling G-men

BODY:

It's ironic that the company the Justice Department worked so hard to break up is crumbling cookies while the government is eating raw meat.

Cookies, as many computer users know, are bits of code that help Web sites keep track of visitors. In addition to innocent uses, cookies have been exploited by hucksters to learn consumers' interests and habits without their knowledge. They're an immeasurable source of personal information.

So, it was welcome news recently when Microsoft Corp. announced new software to allow the individual user to block some or all of these tempting little tastes of their private lives.

In the news about the same time was the FBI's revelation that for the past 18 months it has been using a computer program called Carnivore, which when installed on the network of an Internet provider can comb millions of e-mail messages. The potential for mischief makes cookies seem like something from Grandma's oven.

This new first cousin to wiretapping is necessary, the FBI says, to keep up with ever-more-sophisticated drug dealers and other criminals.

The question is, how do we make sure the authorities are riffling through cybercorrespondence from actual or probable crooks and not the e-files of innocent citizens, members of unpopular groups or political enemies of someone in power?

Pressed by lawmakers, civil libertarians and privacy advocates, the Clinton administration has promised to develop guidelines for bringing consistency and control to e-mail surveillance. (Is there a chance Vice President Al Gore's missing fund-raising e-mails might turn up in the process?)

A major sticking point is the degree of say that Internet providers, standing in for their customers, would have. Clearly, the FBI would prefer to monitor e-mail traffic, with court permission, on its own terms with its own filtration. Privacy groups and some of the providers suggest instead that the feds obtain a court order asking the companies for specific material on a case-by-case basis.

Sounds reasonable. Justifying intrusion prior to the intrusion would not hobble law enforcement and would reassure the overwhelming majority who use the Internet without criminal intent that a large Carnivore was not following their trail of cookie crumbs.

Reprinted from the Indianapolis Star.

SMOLAN-CNS-SD-07-27-00 0703PST
LANGUAGE: ENGLISH

LOAD-DATE: July 28, 2000

Newsbytes

July 28, 2000, Friday

LENGTH: 473 words

HEADLINE: Barr Introduces Legislation To Kill Carnivore

BYLINE: David McGuire; Newsbytes

DATELINE: WASHINGTON, D.C., U.S.A.

BODY:

Hoping to permanently pull the plug on the FBI's controversial e-mail surveillance device, Carnivore, Rep. Bob Barr, R-Ga., on Thursday introduced legislation that would curtail law enforcers' rights to monitor the activity of Internet users.

As he promised earlier this week, Barr introduced the Digital Privacy Act of 2000, which updates federal wiretapping laws to "bring them in line with technological developments such as the Internet, wireless phones and electronic mail," Barr's office said in a statement today.

Specifically, the legislation would prevent the FBI and other law enforcers from accessing individuals' computer files unless "factual evidence reasonably indicates that a crime has been, is being or will be committed."

Electronic evidence illegally obtained by law enforcers would be barred from use in court under the legislation.

Barr's legislation is the latest and most tangible attack on Carnivore, which has been drawing broad-based criticism since news of its use was made public earlier this month.

Designed to attach directly to an Internet service provider's internal systems, Carnivore is capable of sifting through vast quantities of e-mail messages to find those that meet investigative specifications of a court order. Messages that don't meet the specific parameters of a given court order - according to the FBI - are never read.

But the revelation that the FBI is sifting through millions of innocent Internet users' e-mail messages has spawned a groundswell of opposition to the device. Conservatives and liberals alike have decried the FBI's use of the device, claiming that using the technology violates constitutionally protected privacy rights.

Under Barr's legislation, the FBI would not be able to sift through the messages of innocent e-mail users in search of criminal evidence.

One of Carnivore's most ardent congressional opponents, Barr on Thursday was one of more than 25 lawmakers who signed a letter to Attorney General Janet Reno demanding that the FBI shelve the device until the constitutional issues surrounding its use are resolved.

"Given the uproar Carnivore has created, and the potential impact reports on Carnivore could have on consumer confidence in the Internet, we urge you to suspend any activity involving the development or use of Carnivore until the serious privacy issues involved have been satisfactorily answered," the lawmakers wrote.

In addition to hamstringing unchecked e-mail surveillance, Barr's legislation would also prevent law enforcers from tracking the movements of

Doc. #50

cell phone users without first obtaining a court order.

Reported by Newsbytes.com, http://www.newsbytes.com .

16:49 CST Reposted 16:52 CST

(20000728/WIRES ONLINE, LEGAL, BUSINESS/PRIVACYDOME/PHOTO)

LANGUAGE: ENGLISH

TYPE: NEWS

LOAD-DATE: July 29, 2000

The News and Observer (Raleigh, NC)

July 28, 2000 Friday,

STATE EDITION

SECTION: NEWS;

Pg. A7;

NATIONAL BRIEFS

LENGTH: 132 words

HEADLINE: Reno won't suspend 'Carnivore' just yet

BYLINE: From Wire Reports

BODY:

Washington, D.C. -- Attorney General Janet Reno said Thursday she will not suspend the FBI's court-approved monitoring of some people's e-mail while the law enforcement program is under review at the Justice Department. "I think that (FBI) agents can still use it" during the review of the FBI's new "Carnivore" system, Reno said at her weekly news briefing.

Reno said it is important "that we be able to explain the process and address the issues raised by the industry, privacy experts and others." She said she hopes "we will be able to address these issues in a thoughtful way and resolve them."

Reno's comments came amid a move in Congress to increase the burden on federal law enforcement agencies to justify monitoring e-mail and other communications.

LANGUAGE: ENGLISH

LOAD-DATE: July 28, 2000

DOC. #51

National Journal's Technology Daily

PM Edition

July 28, 2000

LENGTH: 238 words

HEADLINE: PRIVACY: Barr To Introduce Digital Privacy Act

BYLINE: Drew Clark

BODY:

Rep. Bob Barr, R-GA, said Friday he would introduce legislation dubbed the Digital Privacy Act that would update wiretapping laws to enhance privacy protections by restricting the police's ability to obtain surveillance information with a warrant issued by a judge.

One provision of the legislation that is similar to a proposal by Sen. Patrick Leahy, D-VT, would give judges discretion over whether or not to authorize wiretaps. Currently, judges must approve such requests so long as a law enforcement officer swears that it is relevant to an ongoing investigation.

Another provision of the bill would overrule a controversial decision last year by the Federal Communications Commission and would stop the government from tracking the location of cell phone users without a court order. "As the White House recently acknowledged, our wiretapping laws have fallen far behind the technological explosion of the past decade," said Barr, a former CIA agent and federal prosecutor. "The Digital Privacy Act corrects some of the most glaring contradictions and loopholes in current law.

As systems from NSA's Echelon spy project to FBI's Carnivore have proven, technological advances make large-scale surveillance easier than ever before. It is vital we safeguard our civil liberties by making certain the law changes to prevent longstanding Fourth Amendment protections from being eroded," Barr said.

LANGUAGE: ENGLISH

LOAD-DATE: July 28, 2000

Doc. #52

(f/k/a Federal Document Clearing House, Inc.)
Congressional Press Releases

July 28, 2000, Friday

SECTION: PRESS RELEASE

LENGTH: 301 words

HEADLINE: BARR BILL UPDATES WIRETAP LAWS

BYLINE: BOB BARR , REPRESENTATIVE , SENATE

BODY: FOR IMMEDIATE RELEASE JULY 27, 20000 BARR BILL UPDATES WIRETAP LAWS MEASURE ENHANCES ELECTRONIC PRIVACY PROTECTION WASHINGTON, D.C. -- U.S. Representative Bob Barr (GA-7) announced today he was introducing the "Digital Privacy Act of 2000." The legislation updates wiretapping laws to enhance privacy protections and bring them in line with technological developments, such as the Internet, wireless phones, and electronic mail.

Specifically, the measure would: > Extend reporting statues requiring law enforcement to report on its interception of electronic communications, in addition to the telephone wiretap reports already required. > Block the use of electronic evidence in court if it is obtained illegally. > Stop unchecked government access to the identities of computer users unless there is reasonable evidence a crime has been committed. > Stop the government from tracking the location of cell phone users without a court order based on probable cause. "As the White House recently acknowledged, our wiretapping laws have fallen far behind the technological explosion of the past decade. For example, under current law, e-mails receive less legal protection than both traditional postal mail and telephone conversations," said Barr. "The Digital Privacy Act corrects some of the most glaring contradictions and loopholes in current law. As systems from NSA's Project Echelon to FBI's Carnivore have proven, technological advances make large scale surveillance easier than ever before. It is vital we safeguard our civil liberties by making certain the law changes to prevent longstanding Fourth Amendment protections from being eroded," Barr continued. Barr, a Member of the House Judiciary Committee, has served with both the Department of Justice and the Central Intelligence Agency.

LANGUAGE: ENGLISH

LOAD-DATE: July 31, 2000, Monday

Doc. #53

The Denver Post

July 28, 2000 Friday

2D EDITION

SECTION: BUSINESS;

Pg. C-04

LENGTH: 867 words

HEADLINE: Soaring online warrants worry privacy advocates

BYLINE: By Will Rodger, USA Today.com,

BODY:

The number of search warrants seeking citizens' online data has soared during the past few years, a USA Today.com study shows.

The findings, based on an examination of search warrants served on the nation's largest Internet service provider, America Online, came as a surprise to federal lawmakers and civil libertarians and are prompting calls for legal reforms.

800 percent jump

The warrants, served by state and local investigators from across the nation, were aimed at discovering the identity and activities of AOL subscribers. In 1997, AOL was served with 33 search warrants, according to court logs in Loudoun County, Va., where AOL is based. That number jumped to 167 in 1998 and 301 in 1999 - an increase of more than 800 percent.

This year, state and local investigators had served 191 warrants on AOL through July 17, the logs show.

Congressional leaders informed of USA Today.com's findings said they will examine legal standards applied to Internet investigations. At a minimum, House Majority Leader Dick Armey, R-Texas, said police need to tell Congress when, why and how they perform electronic searches.

Critics are concerned because they believe that electronic surveillance of all types is a highly powerful tool that, if not tightly controlled, violates rules against unreasonable police searches.

'We do have reports on wiretaps,' Armey said. 'Why shouldn't people have a right to know what the government is doing to access personal correspondence in any media?'

Armey's displeasure echoes the criticism members of a House subcommittee expressed this week about the FBI's new 'Carnivore' Internet wiretapping device. Some say the FBI may be intercepting too much e-mail when it tries to nab messages still in transit from one Net user to another.

But privacy advocates say that while official Washington occupies itself with the legality of Carnivore's real-time e-mail interception, it is ignoring another, possibly more important point: The e-mail stored in online accounts after messages have been delivered has only a fraction of the protections afforded an ordinary telephone call or e-mail still in transit.

Searches for online data typically involve cases ranging from harassment and child pornography to violent crime and fraud.

Doc. #54

White House chief of staff John Podesta has pledged the administration would move soon to protect electronic data.

'Data transmitted over networks is not afforded the full privacy protection we give to traditional phone calls,' he said. 'Considering the extent to which our electronic correspondence contains our most sensitive thoughts and information, shouldn't they count, as (U.S. Supreme Court Justice) Louis Brandeis foreshadowed more than 70 years ago, as the papers and effects mentioned in the Fourth Amendment?'

FBI downplays concerns

FBI officials say there is little reason for concern that stored e-mail and other online records are not as confidential as a personal telephone call.

FBI assistant general counsel Thomas Gregory Motta said the law has treated stored records like e-mail the same way it handles other documents such as letters and diaries, which can be seized from a home with a simple search warrant. 'What about records of my transactions at a bank?' he said. 'I can get that with a subpoena from a grand jury.'

What authorities are looking for can vary by case. In some instances, the logs show, police ask for and get limited information from AOL, such as subscriber identity, billing data and payment history.

Other times police request all such information, plus e-mail; the online 'handles' and names of people cataloged in members' 'buddy lists;' all files attached to e-mail; and all other information contained about the subscriber in the America Online databases.

To comply with the more extensive orders, experts say, AOL must hand over a great deal.

'They can get all information,' said Mark Rasch, a former federal prosecutor and vice president for cyber law at Global Integrity. 'They can get your credit card data and everything you've filed with them. They can get a record of what times you dialed in, where you dialed in from, how long you were online, what activities you were engaged in, what Web sites you visited, what chat sessions you were in and what you said there.'

Internet service companies are privy to everything their members do online. But ISPs vary greatly in their record-retention policies. Some ISPs may keep e-mail for two years or more. Others may delete them after a few weeks. And that will affect authorities' ability to get what they want in criminal investigations.

For instance, he said, companies that host Web sites often keep records of the numeric Internet addresses that hit their sites for years, yet only the visitor's ISP can disclose which subscriber is behind that number.

America Online spokesman Nicholas Graham said the company had no comment on law enforcement's growing interest in subscriber records.

LOAD-DATE: July 31, 2000

International Herald Tribune (Neuilly-sur-Seine, France)

July 28, 2000, Friday

SECTION: Opinion; Pg. 10

LENGTH: 560 words

HEADLINE: Wiretapping in Cyberspace

BYLINE: New York Times Service

BODY:

Millions of people now log on to the Internet as naturally and frequently as they pick up a phone. Technology has created a revolution in personal communications, but technology is also making it possible for government and even employers to monitor private conversations as never before. Telephone-era laws must be updated to address these new challenges to privacy.

Last week the White House proposed some limited changes to theU.S. wiretap and electronic privacy laws that would raise legal standards for government interception of e-mail. Separately, several lawmakersintroduced legislation to require employers to notify employees abouthow e-mail, Internet use and phone calls are monitored.

Employees of The New York Times Co. are already notified that the company reserves the right to reviewe-mail messages while investigating a complaint. Last year the company dismissed 23 employees - most based at a regional business office - for sending offensive e-mail messages.

In the absence of more stringent controls, law enforcement agencies may be tempted to conduct wholesale monitoring of digital written communications. New technology is making it possible for agencies like the FBI to scan, read and record millions of pieces of e-mail on the network of an Internet service provider. Until now this kind of power and its potential for abuse were not so readily available.

Current U.S. wiretapping laws were not drafted with this technology in mind and need to be updated. Various statutes now set different legal standards for the secret interception of domestic communications by law enforcement agencies, depending on whether the communication is by telephone, e-mail or cable modem. The Clinton administration is proposing to eliminate these inconsistencies. Its plan would bring the standards used for intercepting e-mail messages up to the stricter, more protective level now applied to telephone wiretaps. Illegal interception of e-mail would result in suppression of the evidence, as is the case now with illegal interception of phone calls.

The administration is also callingfor greater authority for courts to review law enforcement requests to use devices that record the phone numbers of incoming and outgoing calls and to track the origins and destinations of e-mail messages.

These changes are clearly needed. But Congress also needs to provide new safeguards against the government's wrongful use of ever more powerful surveillance technology against law-abiding citizens. Serious concerns have been raised about Carnivore, the new online wiretap system used by the FBI to track the communications of individuals suspected of criminal activity. The system, when hooked up to the network of the Internet service provider, gives the FBI unlimited access to the e-mail of all subscribers on the network. While a court order is still required to intercept the content of messages, the secret technology controlled exclusively by law enforcement raises fears

Doc #55

of improper monitoring.

Until now, routine government surveillance of private conversations was limited as much by practicality as by legal constraints. Now that it is feasible to eavesdrop electronically on an unlimited scale, the laws have to be strengthened to prevent monitoring of all online communications simply because technology makes it easy.

LANGUAGE: ENGLISH

LOAD-DATE: July 28, 2000

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc #8, OGC FRONT OFFICE FILE (PGS. 8+9)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #56 (Pages 812-813)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

FEDERAL BUREAU OF INVESTIGATION
OFFICE OF PUBLIC AND CONGRESSIONAL AFFAIRS
WASHINGTON, D.C.

TO: Marcus TEL: _____

FAX: 703-632-6081

FROM: Jay TEL: _____

FAX: _____

DATE: 7/27

NO OF PAGES (EXCLUDING COVER): 4

CONTENTS/NOTE:

FYI

Doc. 57

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

3 Pages were not considered for release as they are duplicative of Doc. #36 OPCA FILE (PGS. 552-554)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages: DOCUMENT # 57, PGS. 2-4 (Pages 815 - 817)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of Doc. #24, OGC FRONT OFFICE FILE (PAGE 15)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages: DOCUMENT #58 (Page 818)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

JUL-25-2000 02:29 202 324 3525 P.01/01

FBI

FUGITIVE PUBLICITY/ NATIONAL PRESS OFFICE

WASHINGTON, D.C.

TO: Marcus Thomas DATE: 7/25/00

ATTENTION:

FROM [redacted] - OPCA

FACSIMILE #_____ COMMERCIAL # 202 [redacted]

64-1
67C-1

( ) URGENT (✓) HAND DELIVER ( ) ROUTINE

SUBJECT: This is a copy of what currently appears on the FBI website relative to Carnivore w/the exception of the graphic on the last page. [redacted] wrote an explanation ~~of the~~ for the graphic - we'd like to add it to the site.

COMMENTS:

If you have no problems w/this please initial & have faxed back to me. OR call - we can discuss. Thanks so much

NUMBER OF PAGES:_____ (Including cover page)

Tel: (202) 324-5348 Fax: (202) 324-3525 Homepage: http://www.fbi.gov

Doc. #59

CARNIVORE Diagnostic Tool

Internet and Data Interception Capabilities Developed by the FBI, Statement for the Record, U.S. House of Representatives, the Committee on the Judiciary, Subcommittee on the Constitution, 07/24/2000, Laboratory Division Assistant Director Dr. Donald M. Kerr

The Nation's communications networks are routinely used in the commission of serious criminal activities, including espionage. Organized crime groups and drug trafficking organizations rely heavily upon telecommunications to plan and execute their criminal activities.

The ability of law enforcement agencies to conduct lawful electronic surveillance of the communications of its criminal subjects represents one of the most important capabilities for acquiring evidence to prevent serious criminal behavior. Unlike evidence that can be subject to being discredited or impeached through allegations of misunderstanding or bias, electronic surveillance evidence provides jurors an opportunity to determine factual issues based upon a defendant's own words.

Under Title III, applications for interception require the authorization of a high-level Department of Justice (DOJ) official before the local United States Attorneys offices can apply for such orders. Interception orders must be filed with federal district court judges or before other courts of competent jurisdiction. Hence, unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offense(s) being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses that are anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence -- not intelligence.

Applications must indicate that other normal investigative techniques will not work or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are limited to 30 days and interceptions must terminate sooner if the objectives are obtained. Judges may (and usually do) require periodic reports to the court (typically every 7-10 days) advising it of the progress of the interception effort. This circumstance thus assures close and ongoing oversight of the electronic surveillance by the United States Attorney's office handling the case. Extensions of the order (consistent with requirements of the initial application) are permitted, if justified, for up to a period of 30 days.

Electronic surveillance has been extremely effective in securing the conviction of more than 25,600 dangerous felons over the past 13 years. In many cases there is no substitute for electronic surveillance, as the evidence cannot be obtained through other traditional investigative techniques.

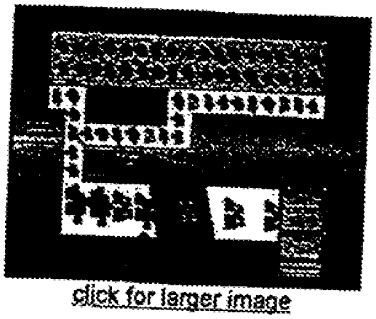
In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims. Because many Internet Service Providers (ISP) lacked the ability to discriminate communications to identify a particular subject's messages to

the exclusion of all others, the FBI designed and developed a diagnostic tool, called Carnivore.

The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept. This type of tool is necessary to meet the stringent requirements of the federal wiretapping statutes.

The Carnivore device works much like commercial "sniffers" and other network diagnostic tools used by ISPs every day, except that it provides the FBI with a unique ability to distinguish between communications which may be lawfully intercepted and those which may not. For example, if a court order provides for the lawful interception of one type of communication (e.g., e-mail), but excludes all other communications (e.g., online shopping) the Carnivore tool can be configured to intercept only those e-mails being transmitted either to or from the named subject.

Carnivore serves to limit the messages viewable by human eyes to those which are strictly included within the court order. ISP knowledge and assistance, as directed by court order, is required to install the device.

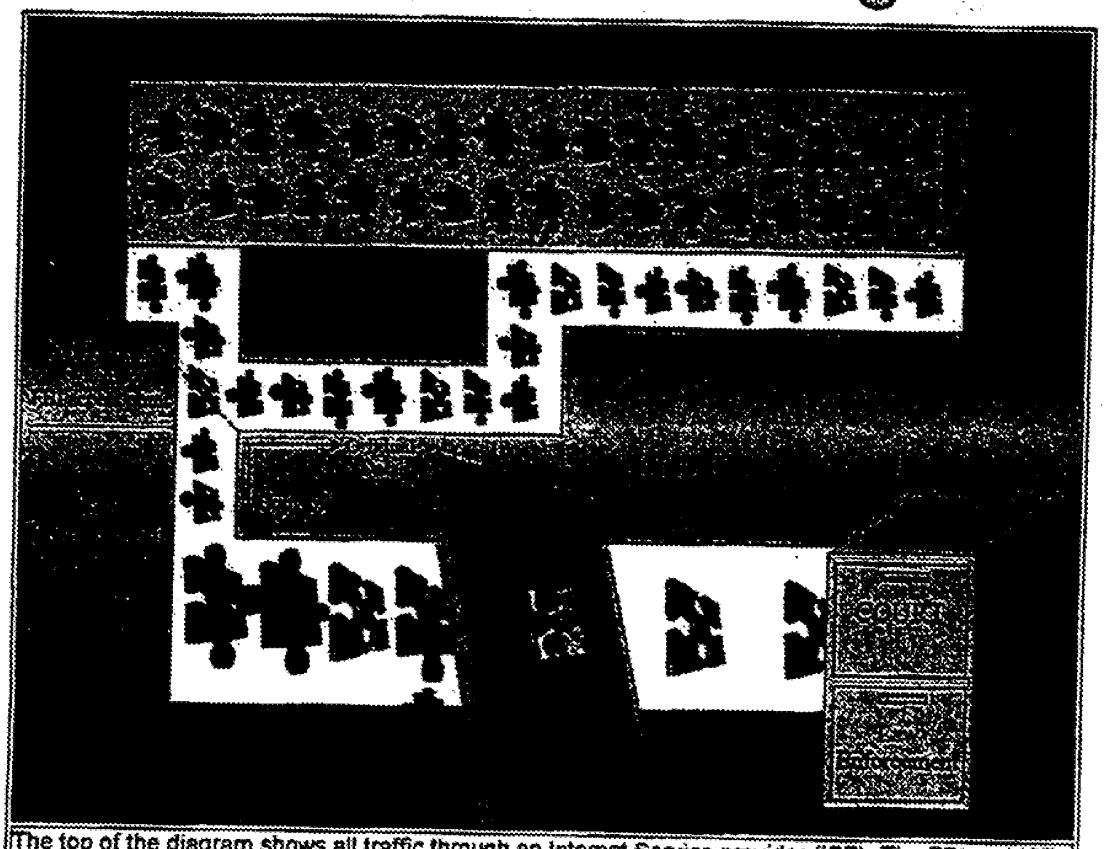


click for larger image

The use of the Carnivore system by the FBI is subject to intense oversight from internal FBI controls, the U. S. Department of Justice (both at a Headquarters level and at a U.S. Attorney's Office level), and by the Court. There are significant penalties for misuse of the tool, including exclusion of evidence, as well as criminal and civil penalties. The system is not susceptible to abuse because it requires expertise to install and operate, and such operations are conducted, as required in the court orders, with close cooperation with the ISPs.

The FBI is sharing information regarding Carnivore with industry at this time to assist them in their efforts to develop open standards for complying with wiretap requirements. The FBI did so two weeks ago, at the request of the Communications Assistance for Law Enforcement Act (CALEA) Implementation Section, at an industry standards meeting (the Joint Experts Meeting) which was set up in response to an FCC suggestion to develop standards for Internet interception.

This is a matter of employing new technology to lawfully obtain important information while providing enhanced privacy protection.



The top of the diagram shows all traffic through an Internet Service provider (ISP). The FBI and ISP work together to identify an access point that contains all traffic from the suspect named in the court order, with as little other traffic as possible. In some cases, the ISP is able to provide the FBI with an access point that contains only the suspect's traffic.

The FBI connects a commercially available one-way tapping device at the ISP's access point. This tap produces an exact copy of all data at the access point. The tap also provides electrical isolation to prevent Carnivore from having any kind of impact on the ISP's network.

The copied network traffic then flows into the collection system where it is compared against a predefined filter. This filter only passes traffic authorized for capture by the court order. Traffic that passes through the filter continues on to be archived to permanent storage media. No other data is ever stored to permanent media, nor is any information recorded about traffic that does not match the filters.

All information available to FBI case agents is also made available to the defense attorneys during the discovery process. In addition, all data stored to permanent media is sealed by the court that issued the court order. In response to a challenge, a judge can order the data to be unsealed and independently analyzed.

Carnivore | Programs and Initiatives | FBI Home Page

To: Finance From: Laboratory
Re: (U) [redacted] (S) 03/07/2000

ECE116, for an amount not to exceed $200,000, and [redacted] (S)

(U) Derived From : G-3
Declassify On: X1

Enclosure(s): (U) Requisition Number 858011.

Details: (U) The Data Intercept Technology Unit, EST-4, is responsible for creating the FBI's Internet intercept devices [redacted] in support of field investigations. An integral part of supporting these collections and capabilities is operational tasking in support of (S) on going and pending [redacted] DRAGONET, [redacted] (S)

b1

(S) [redacted] (S)

TABLE 1: Proposed Funded Amounts by Program

PROGRAM	AMOUNT
[redacted] (S)	[redacted] (S)
DRAGONET	$200,000
[redacted] (S)	[redacted] (S)
[redacted] (S)	[redacted] (S)
TOTAL	[redacted] (S)

(Rev. 10-01-1999)

SECRET

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/07/2000

To: Finance

Attn: [redacted] Room [redacted]
[redacted] Room [redacted]
(Enclosure)
[redacted] Room [redacted]
[redacted] Room [redacted]
Room [redacted]
(enclosure)
Mr. McDevitt, Qt ERF
Mr. Thomas, QT ERF
[redacted] QT ERF
[redacted] QT ERF
QT ERF
QT ERF
QT ERF
(enclosure)
[redacted] QT ERF
(enclosure)
[redacted] QT ERF
(enclosure)

b6-1
b7C-1

National Security

Laboratory

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

From: Laboratory
Electronic Surveuillance Technology Section, EST-4
DITU, QT ERF
Contact: [redacted] (703) [redacted]

b6-1
b7C-1

Approved By: Kerr Donald M
Allen Edward L
McDevitt Michael J
Thomas Marcus C

MAR 2 0 2000

CLASSIFIED BY: AUC39677 SAH/CH
REASON: 1.5 (e,g)
DECLASSIFY ON: X 1

Drafted By: [redacted] llp

b6-1
b7C-1

Case ID #: X [redacted] (S)

Title: X [redacted] (S)

b1

Synopsis: X To request that the Contract Review Unit (CRU) approve and initiate an interim contract [redacted] for a [redacted] This tasking is to be funded under [redacted] BI number JVVCRI

b4-1

(S)

b1

(S)

SECRET

DOC. #60

b1

To: Finance From: Laboratory
Re: (U) [redacted] (S) 03/07/2000

(S) [redacted] (S)

(U) DRAGONET is the program responsible for reactively developing Internet intercept capabilities and developing the capabilities to process the collected data. The sub tasking in this interim contract will include the following: 1) CARNIVORE developments, and 2) Communication protocol developments. (U)

(S) [redacted] (S)

b1

(S) [redacted] (S) and, 2) the (S) augmentation of operational support for the [redacted] The processing and modifications will include but not be limited to the exploration of utilizing a standalone data recording on the [redacted] that allows full system configuration.

(U) Requisition number 858011 is available for this procurement action and funding is available under [redacted] BI number JVVCRP, ECB116 for an amount not to exceed $200,000. (S)

(U) The EST-4 and EST-5 program areas as described above would like to request the that the Engineering Contracts Unit (ECU) approve and initiate an interim contract to be awarded [redacted] and issue a purchase order for [redacted] for the tasking as described in this memo. This matter has been coordinated with [redacted] NS-5A and [redacted] NS-5B. (S)

b4-1
b1
b6-1
b7C-1

To: Finance From: Laboratory
Re: (X) [redacted] 03/07/2000

LEAD(s):

Set Lead 1:

FINANCE

AT WASHINGTON, DC

(U) That the CRU initiate an interim contract to [redacted] in support of the [redacted] DRAGONET, and [redacted] programs.

Set Lead 2:

LABORATORY

AT WASHINGTON, DC

(U) For information only.

Set Lead 3:

NATIONAL SECURITY

AT WASHINGTON, DC

(U) For information only.

♦♦

(Rev. 10-01-1999)

SECRET

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/15/2000

To: Finance

Attn: [redacted] Room [redacted]
[redacted] Room [redacted]
(Enclosure)
[redacted] Room [redacted]
Mr. McDevitt, QT ERF
Mr. Thomas, QT ERF
[redacted] QT ERF
[redacted] QT ERF
(Enclosure)
[redacted] QT ERF
(Enclosure)
[redacted] QT ERF
(Enclosure)
[redacted] QT ERF
(Enclosure)
[redacted] QT ERF
(Enclosure)

Criminal Investigative
Laboratory

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

b6-1
b7C-1

From: Laboratory
Electronic Surveillance Technology Section, EST-4
DITU, QT ERF
Contact: [redacted] (703) [redacted]

b6-1
b7C-1

Approved By: Kerr Donald M
Allen Edward L
McDevitt Michael J
Thomas Marcus C

MAR 2 0 2000 AUC 39677

Drafted By: [redacted] llp

b6-1
b7C-1

CLASSIFIED BY: SAH/cH
REASON: 1.5 (e,g)
DECLASSIFY ON: X

Case ID #: X [redacted](S) b1
268-HQ-1092598 (Pending)

Title: X [redacted](S) DRAGONNET b1

Synopsis: X The Data Intercept Technology Unit (DITU) is requesting that the Contract Review Unit (CRU) add [redacted](S) to [redacted] contract presently being negotiated. This funding is to support development efforts for lawfully authorized Title III Internet Collections. This tasking is to be funded under [redacted](S)

b4-1
b1

b1

SECRET

Doc #61

To: Finance From: Laboratory
Re: (S) [redacted] 03/15/2000

b1

[redacted]

(U) Derived From : G-3
Declassify On: X1

Enclosure(s): (U) Requisition Number 858017.

Details: (S) The Data Intercept Technology Unit, EST-4, is responsible for creating the FBI's Internet intercept devices [redacted] in support of field investigations. An integral part of supporting these collections and capabilities is operational tasking in support of on going and pending [redacted] DRAGONET, [redacted]

(S) [redacted]

b1

(S) [redacted]

TABLE 1: Proposed Funded Amounts by Program

PROGRAM	AMOUNT
[redacted]	[redacted]
DRAGONET	$200,000
[redacted]	[redacted]

To: Finance From: Laboratory
Re: [redacted] 03/15/2000

b1

[redacted]	[redacted]
TOTAL	[redacted]

(S) [redacted]

(S) [redacted]

(S) [redacted]

(S) [redacted] and, 2) the [redacted] The processing and modifications will include but not be limited to the exploration of utilizing a standalone data recording on the [redacted] that allows full system configuration.

(X) Requisition number 858011 is available for this procurement action and funding is available [redacted]

(X) The EST-4 and EST-5 program areas as described above would like to request the that the Engineering Contracts

To: Finance From: Laboratory
Re: [redacted] 03/15/2000 61

(S)

64-1 Unit (ECU) approve and initiate an interim contract to be awarded
61 [redacted] and issue a purchase order for [redacted]
for the tasking as described in this memo. This matter (S)
has been coordinated with [redacted] NS-5A and [redacted]
66-1 [redacted] NS-5B.
67C-1

To: Finance From: Laboratory
Re: [redacted] 03/15/2000

LEAD(s):

Set Lead 1:

FINANCE

AT WASHINGTON, DC

(U) That the CRU initiate an interim contract to [redacted] for [redacted] in support of the [redacted] DRAGONET, and [redacted] programs.

Set Lead 2:

LABORATORY

AT WASHINGTON, DC

(U) For information only.

Set Lead 3:

NATIONAL SECURITY

AT WASHINGTON, DC

(U) For information only.

♦♦

(Rev. 10-01-1999)

SECRET

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/15/2000

To: Finance

Attn: [redacted] Room [redacted]
Room [redacted]
(Enclosure)
[redacted] Room [redacted]
Room [redacted]
Room [redacted]
(enclosure)
[redacted] QT ERF
QT ERF
QT ERF
QT ERF
QT ERF
(enclosure)
[redacted] QT ERF
(enclosure)
[redacted] QT ERF
(enclosure)

National Security

Laboratory

b6-1
b7c-1

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

From: Laboratory
Electronic Surveuillance Technology Section, EST-4
DITU, QT ERF
Contact: [redacted] (703) [redacted]

b6-1
b7c-1

Approved By: Kerr Donald M
Allen Edward L
McDevitt Michael J
Thomas Marcus C

[redacted]

b6-1
b7c-1

Drafted By: [redacted] llp

Case ID #: X [redacted] (S) b1

Title: X [redacted] (S) b1

11-15-2000 AUC 29677
CLASSIFIED BY: SAH:SKS
REASON: 1.5 (c,g)
DECLASSIFY ON: X 1
CV 01849

Synopsis: (U) To request that the Contract Review Unit (CRU) approve and initiate an interim contract with [redacted] for a

b4-1

(U) ~~Derived From : G-3~~
~~Declassify On: X1~~

SECRET

Doc #62

To: Finance From: Laboratory
Re: (X) [redacted] (S) 03/15/2000

61

[redacted] (S) This tasking is to be funded under [redacted] BI number JVVCRP (S) ECE116, for an amount not to exceed $200,000, and [redacted] (S)

Enclosure(s): (U) Requisition Number 858011.

Details: (X) The Data Intercept Technology Unit, EST-4, is responsible for creating the FBI's Internet intercept devices [redacted] in support of (S) field investigations. An integral part of supporting these collections and capabilities is operational tasking in support of on going and pending [redacted] (S) DRAGONET, [redacted] (S)

61 (S) [redacted] (S)

TABLE 1: Proposed Funded Amounts by Program

PROGRAM	AMOUNT
[redacted] (S)	[redacted] (S)
DRAGONET	$200,000
[redacted] (S)	[redacted] (S)
[redacted] (S)	[redacted] (S)
TOTAL	[redacted] (S)

To: Finance From: Laboratory
Re: (X) [redacted] (S) 03/15/2000

(S) [redacted]

(X) DRAGONET is the program responsible for reactively developing Internet intercept capabilities and developing the capabilities to process the collected data. The sub tasking in this interim contract will include the following: 1) CARNIVORE developments, and 2) Communication protocol developments. (U)

(S) [redacted]

(S) [redacted] 2) the [redacted] (S) The augmentation of operational support for the [redacted] processing and modifications will include but not be limited to the exploration of utilizing a standalone data recording on the [redacted] that allows full system configuration.

(X) Requisition number 858011 is available for this procurement action and funding is available [redacted] (S) BI number JVVCRP, ECE116 for an amount not to exceed $200,000, [redacted] (S)

(X) The EST-4 and EST-5 program areas as described above would like to request the that the Engineering Contracts Unit (ECU) approve and initiate an interim contract to be awarded [redacted] and issue a purchase order for [redacted] (S) for the tasking as described in this memo. This matter has been coordinated with [redacted] NS-5A and [redacted] NS-5B.

To: Finance From: Laboratory 61
Re: [redacted] (S) 03/15/2000

LEAD(s):

Set Lead 1:

FINANCE

AT WASHINGTON, DC

64-1 [redacted] for [redacted] That the CRU initiate an interim contract to [redacted] (S) in support of the DRAGONET, and [redacted] programs. [redacted] (S) 61

Set Lead 2: 61

LABORATORY

AT WASHINGTON, DC

(U) For information only.

Set Lead 3:

NATIONAL SECURITY

AT WASHINGTON, DC

(U) For information only.

♦♦

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

18 Page(s) withheld for the following reason(s): PREVIOUSLY PROVIDED TO PLAINTIFF AS PART OF RELEASE #3

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #C3 STATEMENT OF WORK DATED MARCH 23, 2000

(Pages 836-853)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Desk 27

(Rev. 10-01-1999)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/24/2000

To: Finance

Attn: [redacted] Rm [redacted]
[redacted] Rm [redacted]
(enclosures)

Laboratory

Mr. Thomas, QT ERF
[redacted] QT ERF
(enclosure)
[redacted] QT ERF
(enclosures)
[redacted], QT ERF
(enclosures)
[redacted] QT ERF
(enclosure)
[redacted] QT ERF
(enclosures)
[redacted]
(enclosures)

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

b6-1
b7C-1

From: Laboratory
Electronic Surveillance Technology Section, EST-4
DITU, QT ERF
Contact: [redacted] (703) [redacted]

b6-1
b7C-1

DRAFT

Approved By: Allen Edward L
McDevitt Michael J
Thomas Marcus C

[redacted]

b6-1
b7C-1

Drafted By: [redacted] llp

Case ID #: ~~(X)~~ [redacted] (5) / 268-HQ-1092598 61

Title: ~~(X)~~ [redacted] (5) / DRAGONET 61

Synopsis: (U) To request that the Contract Review Unit (CRU) modify the existing FY2000 contract with [redacted] and issue a purchase order for a total amount of $1,045,000. 64-1

(U) ~~Derived From~~ : G-3
~~Declassify On~~: X1

Enclosure(s): (U) 1) Requisition number 858017 for $1,045,000,

~~SECRET~~

8-24-00 AUC39677
CLASSIFIED BY: SAH/JS/CH
REASON: 1.5 (9)
DECLASSIFY ON: X1

Doc #64

To: Finance From: Laboratory
Re: [redacted] 03/24/2000

Details: (U) The DRAGONET Program is the FBI Title III Internet intercept program. This program is responsible for developing the capability of supporting lawfully authorized Internet packet captures in support of law enforcement requirements. This highly specialized collection technology has been developed [redacted] under the codename CARNIVORE. To support the CARNIVORE system which can intercept this traffic is needed. To reduce the cost of this effort, a modification to the [redacted] system will be made. The [redacted] system was originally developed for the [redacted] program and has the capabilities needed by the Dragonet program.

(U) the DRAGONET program is also developing ???(700K)

(U) The Threat Analysis Program has a need for continuing [redacted] support. [redacted] has provided and is supporting an operational database that tracks field operations for EST-4, EST-5, NSD, and the field. The continued operation of this database is critical to operational ERF and field personnel.

(U) A new contract is currently being negotiated with [redacted] for Fiscal year 2000. Please reference electronic communication, titled [redacted] Contract initiation", and dated 11/10/99 for the details of this new contract. The tasking's and funding detailed in the EC is for funding under this new contract.

(U) EST-4 would like to request additional FY2000 funding be transferred to [redacted] to address the following three program areas as delineated in the following table and detailed below.

(U) TABLE 1: Funding Amount By Program

PROGRAM AREA	AMOUNT
1.0 Dragonet - [redacted] Production	$320,000
2.0 Dragonet - ??	$700,000
3.0 Threat Analysis Program	$25,000
TOTAL	$1,045,000

To: Finance From: Laboratory
Re: (X) [redacted] (S) 03/24/2000

(U) Task 1.0 DRAGONET Program Funding - [redacted] (S) PROCUREMENT:

61

(S) Dragonet has an immediate need for the production of the [redacted] (S)

(X) The contractor shall provide a cost estimate for the production of [redacted] (S)

(U) Task 2.0 DRAGONET Program - ???

(U) Task 3.0 Threat Analysis Program

(U) The contractor shall provide software upgrade installation support and software maintenance for the Technical Threat Analysis database and the Special Projects database. The contractor shall supply a software engineer, with an anticipated minimum level of EL-4, to support this effort at a rate of twenty five(25) hours per month.

(U) LOCATION OF WORK

(U) Due to space limitations in the Engineering Research Facility (ERF), it will not be possible to perform all services at the ERF's facility. Accordingly, the Contractor must be prepared to conduct operations in an external location selected by them. FBI reserves the right to approve any such external facilities should a contingency arise.

IX. (U) GOVERNMENT FURNISHED EQUIPMENT

(U) The Government will furnish hardware, applicable documentation and additional GFE requirements that should be identified by the contractor in his proposals.

X. (U) PROGRAM MANAGEMENT

To: Finance From: Laboratory 61
Re: (U) [redacted] 03/24/2000 (5)

(U) To provide managerial and administrative support for the FBI's programs. Scheduling, task assignments and budgets shall be generated. Monthly status reports and other relevant FBI Program Management Office (PMO) documentation shall be [redacted] applied to the FBI Contracting Officer's Technical Representative (COTR) at required intervals. These reports are to include monthly progress during the previous period and expected progress for the following monthly period. Budgeting information, including expenditures to date is to be provided to the FBI on a monthly basis. As part of the contractors program management responsibilities, the contractor shall inform the FBI's Contracting Officer (CO) and Contracting Officer's Technical Representative (COTR), in writing, when any of the tasks reach a seventy percent (70%) spending level. The contractor shall also provide a cost analysis of the remaining funds and time requirements that show the remaining funds are sufficient or insufficient for completing the task.

SECRET

To: Finance From: Laboratory
Re: [redacted] 03/24/2000

LEAD(s):

Set Lead 1:

FINANCE

AT WASHINGTON, DC

(U) That the ECU increase the funding for the FY 2000 [redacted] contract by $1,045,000 for fiscal year 2000, in support of the Dragonet and Technical Threat Analysis programs.

Set Lead 2:

LABORATORY

AT WASHINGTON, DC

(U) For information only.

Set Lead 3:

NATIONAL SECURITY

AT WASHINGTON, DC

(U) For information only.

♦♦

SECRET

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

20 Page(s) withheld for the following reason(s): PREVIOUSLY PROVIDED TO PLAINTIFF AS PART OF RELEASE #3

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #65, STATEMENT OF WORK DATED MARCH 24, 2000
(Pages 859-878)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

01/3/01

SECRET

STATEMENT OF WORK

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

(U) STATEMENT OF WORK FOR FY 2000

(ADDITIONAL TASKING)

64-1 [redacted]

b1 [redacted] (S)

DRAGONET THREAT ANALYSIS PROGRAM

June 1, 2000

MAR 2 0 2002 Auc 39677
CLASSIFIED BY: SAH/CL
REASON: 1.5 (e,g)
DECLASSIFY ON: X 1

(U) Derived From : G-3
Declassify On: X1

SECRET

Doc. #66

STATEMENT OF WORK

STATEMENT OF WORK

[redacted] b4-1 [redacted]

TABLE OF CONTENTS

STATEMENT OF WORK

I. (U) INTRODUCTION

64-1

(S) [redacted] has been and is currently being tasked with [redacted] software and [redacted] This SOW will incorporate additional tasking and tasking modifications for the current FY 2000 contract J-FBI-00-080. (S)

61

II. (U) PROJECT DESCRIPTION BY TASKING AREAS

64-1

(U) The [redacted] tasking (Tasking numbers are referenced to the original contract tasks):

64-1

(U) TABLE 1: [redacted] Tasking Area Summary Table

TASKING AREA #	TASK DESCRIPTION
2.8	RENAMING TASK
2.14	(S) [redacted] TASKING
4.3	DRAGONET - [redacted] (S)
4.4	DRAGONET - High Speed Intercept Study
6.0	Technical Threat Analysis Program - Data Base Support

61

(U) Sections III, IV, V, VI, and VII give a more detailed description of the tasking for FY2000.

III. (U) TASKING 2.8 - HAWKING ROUTER ENHANCEMENTS :

(U) This task has been renamed **VIKING ENHANCEMENTS.**

61

IV (U) TASKING 2.14 - [redacted] (S) TASKING :

61

(S) [redacted] (S)

V. (U) TASKING AREA #4.3 - [redacted] (S)

(S) [redacted]

b1 [redacted]

VI. (U) TASKING AREA #4.4 HIGH SPEED INTERCEPT STUDY

b1 (S) [redacted] This task shall provide the DRAGONET program with a capability for Internet data interception. The contractor shall make enhancements to existing Carnivore intercept drive overall system throughput performance. These enhancements will make use operating system performance enhancements to include service pack 1 with additional capability that will be added in addition to overall throughp Carnivore to filter on PPP streams and the update of the graphical user filter associated with PPP.

VII. (U) THREAT ANALYSIS PROGRAM

STATEMENT OF WORK

(U) The contractor shall provide software upgrade installation support and software maintenance support for the Technical Threat Analysis database and the Special Projects database. The contractor shall supply a software engineer, with an anticipated minimum level of EL-4, to support this effort at a rate of twenty five (25) hours per month.

VIII. (U) LOCATION OF WORK

(U) Due to space limitations in the Engineering Research Facility (ERF), it will not be possible to perform all services at the ERF's facility. Accordingly, the Contractor must be prepared to conduct operations in an external location selected by them. FBI reserves the right to approve any such external facilities should a contingency arise.

IX. (U) GOVERNMENT FURNISHED EQUIPMENT

(U) The Government will furnish hardware, applicable documentation and additional GFE requirements that should be identified by the contractor in his proposals.

X. (U) PROGRAM MANAGEMENT

(U) To provide managerial and administrative support for the FBI's programs. Scheduling, task assignments and budgets shall be generated. Monthly status reports and other relevant FBI Program Management Office (PMO) documentation shall be generated and supplied to the FBI Contracting Officer's Technical Representative (COTR) at required intervals. These reports are to include monthly progress during the previous period and expected progress for the following monthly period. Budgeting information, including expenditures to date is to be provided to the FBI on a monthly basis. As part of the contractors program management responsibilities, the contractor shall inform the FBI's Contracting Officer (CO) and Contracting Officer's Technical Representative (COTR), in writing, when any of the tasks reach a seventy percent (70%) spending level. The contractor shall also provide a cost analysis of the remaining funds and time requirements that show the remaining funds are

sufficient or insufficient for completing the task.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

4 Page(s) withheld for the following reason(s): RESPONSIVE PAGES FROM THIS REPORT WERE PART OF RELEASE #5

☒ The following number is to be used for reference regarding these pages:
DOCUMENT 67, FY 2000 TECHNICAL PROPOSAL
(Pages 885-888)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

(Rev. 10-31-1999)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/16/2000

To: Finance **Attn:** Mr. Stollhans, Room 6032
[redacted] Room [redacted]
(Enclosure)

[redacted] Criminal Investigative 66-1
67C-1
Laboratory [redacted] Room [redacted]
(Enclosure)
Mr. Thomas, QT ERF
[redacted] QT ERF
[redacted] QT ERF
[redacted] QT ERF
(Enclosure)

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

From: Laboratory
Cyber Technology Section,
Data Intercept Technology Unit, QT ERF
Contact: SSA [redacted] (703) [redacted] 66-1 67C-1

Approved By: Kerr Donald M
Allen Edward
Thomas Marcus
[redacted] 66-1 67C-1

Drafted By: [redacted] llp

Case ID #: 268-HQ-1092598 (Pending)

Title: DRAGONNET

Synopsis: Request of the Finance Division to assign funding for requisition number 827303 from budget line item ETX122, in the amount of $347,730, modifying contract J-FBI-00-080 [redacted] 64-1 Inc.

Enclosure(s): Enclosed for Finance is Requisition number 827303.

Details: Requisition number 827303 is being submitted to modify the existing contract number J-FBI-00-080, [redacted] The 64-1 modification consists of increasing the original contract by $347,730. The additional funding will provide for one Senior Engineer, for a one year period, to support deployment of Internet Interception and Collection systems. This task will consist of supporting system deployments

61 [redacted]

(S)

MAR 20 2001
CLASSIFIED BY: Auc 39677 SAH/cdh
REASON: 1.5 (e,g)
DECLASSIFY ON: X1

~~SECRET~~

Doc. #68

SECRET

This modification will also provide additional funds to the operational support task [redacted] (S)

b1

The Contracting Officer is [redacted] The Program Leader is [redacted] The COTR is [redacted]

b6-1
b7C-1

SECRET

~~SECRET~~

LEAD(s):

Set Lead 1 (Adm)

FINANCE

[redacted]

AT WASHINGTON, DC

The Finance Division is requested to modify Contract Number J-FBI-00-080.

Set Lead 2 (Adm)

CRIMINAL INVESTIGATIVE

AT WASHINGTON, DC

64-1 To approve funding for requisition number 827303 from budget line item ETX122, in the amount of $347,730, modifying contract J-FBI-00-080 [redacted]

Set Lead 3 (Adm)

LABORATORY

AT QUANTICO, VA

For information only.

♦♦

~~SECRET~~

DRAFT

REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

SECRET

[redacted] (FOUO) (S)

[redacted] (FOUO) (S)

[redacted] (FOUO) (S)

61

[redacted] (FOUO) (S)

SENSITIVE ELECTRONIC SURVEILLANCE TECHNIQUE INFORMATION INCLUDED
DO NOT DISCLOSE

SECRET

~~SECRET~~

DRAFT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

- Should be in the form of a memo from the Director to the AG. May 5, 2000
- Should be classified ~~SECRET~~.
- Has NSLU reviewed?

MAR 2 0 2002

AUC 39477

CLASSIFIED BY: SAHlcH
REASON: 1.5 (e,g)
DECLASSIFY ON: X 1

REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

[redacted] (S)

[redacted] (S)

[redacted] (S)

[redacted] (S)

[redacted] (FOUO)

[redacted] (S)

b1

SENSITIVE ELECTRONIC SURVEILLANCE TECHNIQUE INFORMATION INCLUDED
DO NOT DISCLOSE

SECRET

Doc. #69

DRAFT

SECRET

REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

[redacted] (S)

[redacted] (S)

Proposed Procedures:

[redacted] (S)

[redacted] (S)

[redacted] (S)

61

3. Non-targeted testing: All FBI testing shall be conducted in such a way that it will not be targeted against the communications of any particular person or persons. (FOUO) (4)

[redacted] (S)

SENSITIVE ELECTRONIC SURVEILLANCE TECHNIQUE INFORMATION INCLUDED
DO NOT DISCLOSE

SECRET

DRAFT

REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

b1 [redacted] (FOUO) (S)

[redacted] (FOUO) (S)

6. Duration: The testing herein shall be limited in extent and duration to that necessary to determine the capability of the equipment, including refining the precision of the equipment. Testing herein shall not exceed 90 days without the prior approval of the Attorney General ~~or designee of the Attorney General~~. ~~(FOUO)~~ (U)

7. Agency Oversight: FBI LD testing herein, including compliance with the procedures set forth herein, shall be closely monitored by the FBI LD's Chief of the Cyber Technology Section. ~~(FOUO)~~ (U)

8. Reporting: Upon completion of the testing herein, the FBI LD shall submit a summary report to the Department of Justice's Office of Intelligence Policy and Review briefly setting forth the results of the testing, stating its compliance with these testing procedures, and identifying the duration of the testing. (U)

b1 [redacted] (S)

SENSITIVE ELECTRONIC SURVEILLANCE TECHNIQUE INFORMATION INCLUDED
DO NOT DISCLOSE

~~SECRET~~

SECRET

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

May 12, 2000

MAR 20 2001 AUC 39677
CLASSIFIED BY: SAH/CA
REASON: 1.5 (c,g)
DECLASSIFY ON: X1

Director:

(S) [redacted]

b1

(S) [redacted]

(S) [redacted]

(S)

(X) After recognizing the efficacy of using these statutorily-based procedures, the LD shared this proposed course of action with the Counterterrorism Division and the Office of the General Counsel, and they acknowledged the usefulness of this (U)

Enclosures (2)

1 - Mr. Pickard, Room 7142
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room 7427

b6-1
b7C-1

ARM:pak (17)

1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - Dr. Kerr, Room 3090
1 - Mr. Allen, QT ERF
1 - Mr. Thomas, QT ERF
1 - [redacted] QT ERF
1 - [redacted] Room [redacted]

(U) Classified by: G-3
Declassify on: X-1

SECRET

5/24/02 Release - Page 896

Doc. #70

approach. Moreover, the LD has shared with the DOJ's Office of Intelligence Policy and Review (OIPR) a draft of the attached proposed memorandum to the Attorney General, which includes the proposed electronic surveillance testing procedures. OIPR supports this "testing" approach, as provided for in the FISA [redacted] and it also supports the specific testing procedures proposed by the LD. (U) See attachment #2).

61

[redacted] (S)

~~(FOUO)~~ If you approve of this approach, the OIPR advises that the FBI request should be forwarded to the Attorney General through the attached memorandum, which the OIPR has already approved in draft form. (U)

Donald M. Kerr

[redacted]

ATTACHMENT 1

SECRET

Memorandum

To : Mrs. Frances Fragos Townsend Date 04/28/2000
Counsel, Office of Intelligence
Policy and Review

From : [redacted]
Dale L. Watson
Assistant Director
Counterterrorism Division

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

Subject : [redacted] (S)

b1

ACTION MEMORANDUM

(S) [redacted] (S)

b1

(S) [redacted] (S) The Carnivore software filters the target's communications from other communications and stores the targeted communications to storage media where the communications can be maintained as evidence.

b6-1
b7C-1

1 - [redacted]
1 -
1 -
1 -
1 -
1 -
1 -
AMK:amk(8)

SEE NOTE PAGE FIVE

Classified by: 4877, ITOS, CTD
Reason: 1.5(C)
Declassify on: X1

MAR 3 0 2002

SECRET

AMC 39677
CLASSIFIED BY: SAH\cd
REASON: 1.5 (c,g)
DECLASSIFY ON: X 1

Mrs. Frances Fragos Townsend
Counsel, Office of Intelligence
Policy and Review
Re: [redacted] (S) b1

[redacted] (S)

(U) The Carnivore software has been developed and tested over a period of years and has been deployed in the field successfully on numerous occasions. However, it has never been installed in the USA.NET network. While most networks use standard protocols, protocols can vary widely from the standards in some networks.

b1

(S) [redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

Mrs. Frances Fragos Townsend
Counsel, Office of Intelligence
Policy and Review
Re: [redacted] (S) b1

b1

(S) [redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

Mrs. Frances Fragos Townsend
Counsel, Office of Intelligence
Policy and Review
Re: [redacted] (S)

61

(S) [redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

SECRET

Mrs. Frances Fragos Townsend
Counsel, Office of Intelligence
Policy and Review

Re: [redacted] (S)

b1

[redacted] (S)

SECRET

ATTACHMENT 2

SECRET

EXECUTIVE SUMMARY

TO: THE ATTORNEY GENERAL

THROUGH: MRS. FRANCES FRAGOS TOWNSEND
COUNSEL, OFFICE OF INTELLIGENCE
POLICY AND REVIEW

FROM: LOUIS J. FREEH
DIRECTOR, FBI

SUBJECT: (U) REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

ACTION MEMORANDUM

PURPOSE: (U) To obtain the Attorney General's approval of the attached FBI electronic surveillance testing procedures pursuant to authority vested in the Attorney General in Section 105(f) of the Foreign Intelligence Surveillance Act of 1978 (FISA), codified at 50 U.S.C. 1805(f).

TIMETABLE: (U) The Attorney General is requested to approve the proposed FBI testing procedures as soon as possible. Testing pursuant to these procedures is essential for the FBI to be able(w)

Classified by: G-3
Declassify on: X-1

MAR 3 0 2002 AUC 39677
CLASSIFIED BY: SAH/dL
REASON: 1.5 (C, G)
DECLASSIFY ON: X 1

SECRET

SECRET

Memorandum to The Attorney General from Director, FBI

[redacted] (S)

b1

[redacted] (S)

RECOMMENDATION: (U) Attorney General approve the attached FBI electronic surveillance testing procedures.

APPROVE _____

DISAPPROVE _____

OTHER _____

Concurring components:

NONE

Nonconcurring components:

NONE

SECRET

SECRET

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

MAR 2 0 2002 Auc 39677

CLASSIFIED BY: SAH\CH
REASON: 1.5 (C,G)
DECLASSIFY ON: X-1

MEMORANDUM FOR THE ATTORNEY GENERAL

THROUGH: MRS. FRANCES FRAGOS TOWNSEND
COUNSEL, OFFICE OF INTELLIGENCE
POLICY AND REVIEW

FROM: Louis J. Freeh
Director, FBI

SUBJECT: (U) REQUEST FOR APPROVAL OF TESTING
OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

ACTION MEMORANDUM

PURPOSE: (U) To obtain the Attorney General's approval of the attached FBI electronic surveillance testing procedures pursuant to authority vested in the Attorney General in Section 105(f) of the Foreign Intelligence Surveillance Act of 1978 (FISA), codified at 50 U.S.C. 1805(f).

TIMETABLE: (X) The Attorney General is requested to approve the proposed FBI testing procedures as soon as possible. Testing pursuant to these procedures is essential for the FBI [redacted] (S)

61 [redacted] (S)

(U) Classified by: G-3
Declassify on: X-1

SECRET

[redacted] (5)

[redacted] (5)

b1

[redacted] (5)

[redacted] (S)

[redacted] (S)

b1

[redacted] (S)

[redacted] (S)

[redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

b1

[redacted] (S)

~~(TOUO)~~ Proposed Procedures:

(S) [redacted] (S)

(S) [redacted] (S)

(X) 2. [redacted] (S)

b1

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

b1 [redacted] Carnivore is an FBI-designed (S) software program that, in important respects, filters and then intercepts with great precision various ISP data elements (including content when authorized) based upon reference to certain standardized ISP TCP/IP protocols.

(S) [redacted] (S)

b1

~~(FOUO)~~ 4. <u>Non-targeted testing</u>: All FBI testing shall be conducted in such a way that it will not be targeted against the communications of any particular person or persons. (U)

b1 [redacted] (S)

b1 [redacted] (S)

~~(FOUO)~~ 7. <u>Duration</u>: The testing herein shall be limited in extent and duration to that necessary to determine the capability of the equipment, including refining the precision of the equipment. Testing herein shall not exceed 90 days without the prior approval of the Attorney General. (U)

~~(FOUO)~~ 8. <u>Agency Oversight</u>: FBI LD testing herein, including compliance with the procedures set forth herein, shall be closely monitored by the FBI LD's Chief of the Cyber Technology Section. (U)

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

~~(FOUO)~~ 9. Reporting: Upon completion of the testing herein, the FBI LD shall submit a summary report to the Department of Justice's Office of Intelligence Policy and Review briefly setting forth the results of the testing, stating its compliance with these testing procedures, and identifying the duration of the testing. (U)

RECOMMENDATION: Attorney General approve the attached electronic surveillance testing procedures. (U)

APPROVE _____

DISAPPROVE _____

OTHER _____

Concurring components:

NONE

Nonconcurring components:

NONE

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

66-1
67C-1

1 - Mr. Pickard, Room 7142
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - Mr. Parkinson, Room 7427
PAK (17)

1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - Dr. Kerr, Room 3090
1 - Mr. Allen, QT ERF
1 - Mr. Thomas, QT ERF
1 - [redacted] Room [redacted]
1 - [redacted] QT ERF

SECRET

Memorandum

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

To : The Attorney General Date 05/11/2000

From : Director, FBI

Subject : (U) REQUEST FOR APPROVAL OF TESTING OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

ACTION MEMORANDUM

b1

(S) [redacted] (S)

(S) [redacted] (S)

[redacted] (S)

MAR 2 0 20[redacted] AUC 39677
CLASSIFIED BY: SAH/cH
REASON: 1.5 (g)
DECLASSIFY ON: [redacted]

SECRET

Doc # 71

Memorandum from Deputy Director to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

[redacted] (S)

[redacted] (S)

[redacted] (S)

[redacted] (S)

b1

Memorandum from Deputy Director to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

[redacted] (5)

b1

[redacted] (5)

(S) [redacted] (5)

(S) [redacted] (5)

b1

~~(FOUO)~~ Proposed Procedures:

(S) [redacted] (5)

(S) [redacted] (S)

b1

2. Testing Equipment: [redacted] (S) Carnivore is an FBI-designed software program that, in important respects, filters and then intercepts with great precision various ISP data elements (including content when authorized) based upon reference to certain standardized ISP TCP/IP protocols.

(S) [redacted] (S)

~~(TOUO)~~ 4. Non-targeted testing: All FBI testing shall be conducted in such a way that it will not be targeted against the communications of any particular person or persons. (U)

[redacted] (S)

Memorandum from Deputy Director to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING, May 11, 2000

b1 [redacted] (5)

[redacted] (5)

~~(FOUO)~~ 7. Duration: The testing herein shall be limited in extent and duration to that necessary to determine the capability of the equipment, including refining the precision of the equipment. Testing herein shall not exceed 90 days without the prior approval of the Attorney General. (4)

~~(FOUO)~~ 8. Agency Oversight: FBI LD testing herein, including compliance with the procedures set forth herein, shall be closely monitored by the FBI LD's Chief of the Cyber Technology Section. (4)

~~(FOUO)~~ 9. Reporting: Upon completion of the testing herein, the FBI LD shall submit a summary report to the Department of Justice's Office of Intelligence Policy and Review briefly setting forth the results of the testing, stating its compliance with these testing procedures, and identifying the duration of the testing. (4)

SECRET

MEMORANDUM FOR THE ATTORNEY GENERAL 6/1/00

THROUGH: MRS. FRANCES FRAGOS TOWNSEND
COUNSEL, OFFICE OF INTELLIGENCE
POLICY AND REVIEW

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

FROM: LOUIS J. FREEH
DIRECTOR, FBI

SUBJECT: (U) REQUEST FOR APPROVAL OF TESTING OF FBI ELECTRONIC SURVEILLANCE EQUIPMENT

ACTION MEMORANDUM

PURPOSE: (U) To obtain the Attorney General's approval of the attached FBI electronic surveillance testing procedures pursuant to authority vested in the Attorney General in Section 105(f) of the Foreign Intelligence Surveillance Act of 1978 (FISA), codified at 50 U.S.C. 1805(f).

TIMETABLE: (U) The Attorney General is requested to approve the proposed FBI testing procedures as soon as possible. Testing pursuant to these procedures is essential for the FBI [redacted] (S)

b1 [redacted] (S)

66F-HQ-1012493

1 - Mr. Pickard, Room 7142
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - Mr. Parkinson, Room 7427
ARM:pak (17)

b6-1
b7C-1

1 - [redacted] Room [redacted]
1 - [redacted] Room [redacted]
1 - Dr. Kerr, Room 3090
1 - Mr. Allen, QT ERF
1 - Mr. Thomas, QT ERF
1 - [redacted] Room [redacted]
1 - [redacted] QT ERF

(U) ~~Classified by: G-3~~
~~Declassify on: X 1~~

SECRET

5/24/02 Release - Page 921

3-20-02 AUC 39677
CLASSIFIED BY: SAH/CM
REASON: 1.5 (c,g)
DECLASSIFY ON: X

Doc #72

[redacted] (S)

[redacted]

b1

[redacted] (S)

[redacted] (S)

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING

[redacted] (S)

[redacted] (S)

[redacted] (S)

[redacted] (S)

b1

[redacted] (S)

(S) [redacted] (S)

(S) [redacted] (S)

b1

[redacted] (S)

~~(FOUO)~~ Proposed Procedures:

(S) [redacted] (S)

(S) [redacted]

b1

(S) 2. [redacted] (S)

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING

[redacted] (S) Carnivore is an FBI-designed software program that, in important respects, filters and then intercepts with great precision various ISP data elements (including content when authorized) based upon reference to certain standardized ISP TCP/IP protocols.

(S) [redacted] (S)

~~(FOUO)~~ 4. Non-targeted testing: All FBI testing shall be conducted in such a way that it will not be targeted against the communications of any particular person or persons. (U)

b1

[redacted] (S)

[redacted] (S)

~~(FOUO)~~ 7. Duration: The testing herein shall be limited in extent and duration to that necessary to determine the capability of the equipment, including refining the precision of the equipment. Testing herein shall not exceed 90 days without the prior approval of the Attorney General. (U)

~~(FOUO)~~ 8. Agency Oversight: FBI LD testing herein, including compliance with the procedures set forth herein, shall be closely monitored by the FBI LD's Chief of the Cyber Technology Section. (U)

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING

~~(FOUO)~~ 9. Reporting: Upon completion of the testing herein, the FBI LD shall submit a summary report to the Department of Justice's Office of Intelligence Policy and Review briefly setting forth the results of the testing, stating its compliance with these testing procedures, and identifying the duration of the testing. (U)

RECOMMENDATION: Attorney General approve the attached electronic surveillance testing procedures. (U)

APPROVE _____

DISAPPROVE _____

OTHER _____

Concurring components:

NONE

Nonconcurring components:

NONE

Memorandum from Director, FBI to The Attorney General
Re: REQUEST FOR APPROVAL OF TESTING